Cortexa TECHNOLOGY

THE AFFORDABLE DIGITAL HOME IS HERE

CORTEXA OWNER'S MANUAL

WWW.CORTEXATECHNOLOGY.COM

Table of Contents

Table of Contents

Continued

Continued

Continued

CONGRATULATIONS

Congratulations on your purchase of a Cortexa Technology Home Automation system. The controller or "brain" of the system is called the Cortexa 7202. This is an integrated hardware and software solution, controlling and managing all of the sub-systems you choose to automate within your home.

This Owners Guide will help you get the most out of the system. We recommend that you read this guide carefully to fully understand the extensive capabilities of the Cortexa Home Automation system.

ORGANIZATION OF THIS OWNERS GUIDE

The layout of this guide is identical to the Configuration Utility page within the Cortexa configuration tool. In organizing the contents in this way, we hope it will be easy for you to locate the subject or function you are looking for. The Configuration Utility page for the Cortexa 7202 is reached by selecting the Tools icon from the Home Page.

SYSTEM CONTENTS

The Cortexa package includes:

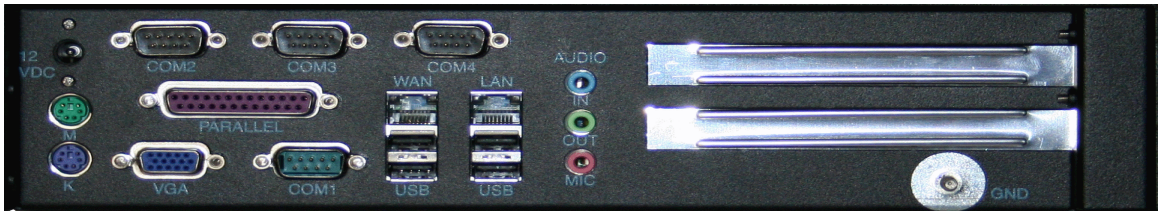
- Cortexa 7202 Home Automation Controller
- Power supply 12VDC, 5 Amp
- CD containing documentation

SYSTEM REQUIREMENTS

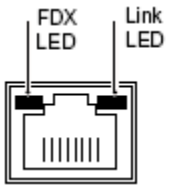
- Broadband Internet (DSL or Cable)
- A Network Switch capable of 10/100 Mbps
- Network cables to connect the broadband modem, Cortexa 7202 and network switch
- PC with Microsoft Internet Explorer 4.0 or later, or similar Internet Browser with JAVA 2.0 support

REAR PANEL

The rear panel of the Cortexa 7202 is shown below.



12VDC	Power 12V DC power connection 12Volt 5 Amp (included)
K	PS2 keyboard connection. Used only to reset the device back to factory defaults
M	Mouse connection. Not used
Com 1,2,3,4	Used to connect sub-systems
USB	Two USB ports. Used to connect to USB-RS232 adapters for further expansion
WAN	Used to connect to a broadband connection (connects to Cable/DSL modem)
LAN	Used to connect to a local area network switch
VGA	Monitor connection. Used only to reset the device back to factory defaults
Parallel	Used to connect an 8-port parallel relay board
Out, In, Mic	Audio connections are used for the built-in Cortexa Audio player
Gnd	Used to ground the Cortexa



All network ports are 10/100 Mbps Ethernet. Each port supports only unshielded twisted pair (UTP) cable using an 8-pin RJ-45 plug with standardized T568A or T568B Terminations. Each port uses RJ-45 connectors that have two LEDs. The network access speed is automatically sensed and displayed by the left or FDX LED color. The right or LINK LED is solid green when properly linked to another network device and blinks during network activity.

Label	Color	Activity	Description
FDX	Green	On	The port is Linked and operating at 100 Mbps
	Yellow	On	The port is Linked and operating at 10 Mbps
Link	Green	Blinking	Packet transmission or reception is occurring on the port

FRONT PANEL

The front panel of the Cortexa 7202 is shown below.

FRW	Indicates flash memory read/write activity
PWR	Power on/off indicator
RST	Resets the Cortexa
PWR SW	Turns the Cortexa on/off. To turn off hold for four seconds

A basic understanding of networking and the connected sub-systems is highly recommended to ensure a smooth installation of this product. All systems connected should be installed according to the respective manufacturer's recommendations.

In addition, ensure qualified personnel are used to install equipment where required. For example, a licensed electrical contractor will be required to install all line voltage devices such as light switches, and a licensed security contractor will be required to install or modify your security system.

The following is an overview of the basic steps in setting up a system for the first time. More detail is provided in the respective sections of this guide. It is important that you follow the steps below in order to ensure the installation goes smoothly.

PRE-WIRING

Ensure all pre-wiring is in place, based on which sub-systems you intend to automate. Pre-wire requirements for all sub-systems are detailed in the Cortexa Pre-Wire Guide, available from www.cortexatechnology.com.

INSTALLING SUB-SYSTEM DEVICES

Physically install all sub-system devices. Here we are talking about security systems, lighting devices, thermostats, irrigation modules, surveillance cameras, audio system.

Be sure to ensure all sub-systems and devices are working satisfactorily before you start integrating them into your Cortexa system.

CONNECTING TO THE CORTEXA 7202

Physically connect the RS232 connector for each of the following sub-systems (Security, Lighting, Irrigation, HVAC, Audio), as applicable in your case, to a Com port on the back on the Cortexa. It does not matter which sub-system connects to which port, however note which port each sub-system is connected to for the next step in the process. The only exception to this is HVAC, which must be configured to Com1 or Com2.

CONNECTING THE CORTEXA TO THE NETWORK

This step establishes the Cortexa to your network and the accessibility to the Internet. In most cases, the Cortexa will come plug and play out of the box, without requiring any network configuration. If this is not the case, refer to Section 4, Initial Network Setup, for more information.

CONFIGURING THE SUB-SYSTEMS

From the Sub-System Setup tab on the Configuration Utility Page, configure each sub-system to the Com port it is physically connected to. Com ports are selected by clicking on the drop down arrow beside the port. This will display all available Com ports. Simply click on the Com port desired and the Cortexa will then recognize that particular sub-system.

SETTING UP THE SUB-SYSTEMS

Within each sub-system, all of its specific devices must then be added to the Cortexa. This is a simple process, and obviously varies by sub-system. Details on how to do this are provided in the section of this Owners Guide pertaining to each sub-system. The following is an overview by sub-system to help explain what information and configuration we are talking about here.

Security:	Security zone information is entered into the Cortexa Security Manager
HVAC:	Each thermostat must be physically configured to have a unique address
Lighting:	Specific lighting devices are configured into Areas (Rooms) in the Cortexa
Irrigation:	Irrigation zones are added to and labeled in the Cortexa
Cameras:	Names associated with each camera are assigned and entered into the Cortexa
Audio:	Zone names and source names are configured
IR Control:	IR codes are learned into the Cortexa, and custom remote controls are configured

WRITING EVENTS

Now that everything is configured in the Cortexa, you are ready to start writing events. This is the fun part, where the system starts to come alive and automate your home. The extent to which you can have the system automate the sub-systems in your home is limited only by your imagination and creativity, so many scenarios are possible.

The way to think about your new integrated home is that every device configured into the Cortexa is "connected" to every other device. So, thermostats, lights, security zones, cameras, audio, TVs/DVDs (through IR control) are "connected" – your vision of living in a connected home is becoming a reality.

Here is one simple example of the integration of the sub-systems. Think about all the things you do when you go to bed at night; arm the security system, turn lights off, check garage doors are closed, adjust thermostat(s), turn TVs and other devices off. With one simple event in the Cortexa, just arming the security system will trigger all of these other things to happen automatically, within seconds.

Event writing is simple; there is no programming language to learn. Events are written using selections provided to you in drop-down boxes and we feel sure you will easily master writing your own events.

Be sure to name your events logically so you can easily identify each event and what each event performs.

There is a detailed section on event writing, including several sample events, in the Home Management section of this Owners Guide.

Continued

SETUP YOUR LOCAL AREA NETWORK (LAN)

Your computer should be connected to a port on a network switch, and the network switch connected to the LAN port of the Cortexa. You will use standard Category 5, or better, cables to do this. The link light for each port will be lit when you are properly connected and all devices are turned on. A direct connection may also be made from the Cortexa LAN to a Computer, however this requires Cat5 crossover cable.

START UP SEQUENCE

1. Power up your broadband modem first and wait approximately one minute for it to complete diagnostics as indicated by the panel lights. If you have been connected to another router previously, make sure to leave the modem power off for 1 to 2 minutes to refresh the router table.
2. After your modem is ready, start the Cortexa by pushing the power button. Wait approximately 2 minutes for the operating system to load.
3. Start your Computer. When ready, open an instance of your preferred Internet browser i.e. Internet Explorer, Mozilla Firefox, etc.

LOGGING INTO THE CORTEXA

The Cortexa factory default settings issue DHCP addresses for the default gateway IP range that is 192.168.10.100 to 192.168.10.150. If your computer is configured to receive a DHCP address then you should have received an address in that range. If it is not configured to receive a DHCP address, then you can manually set your IP address. Defaults for manual TCP/IP configuration are as follows:

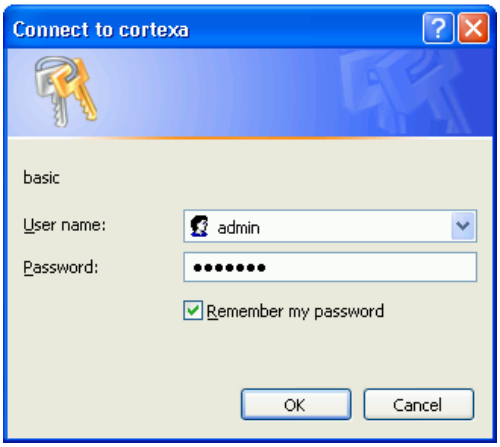
IP Address	192.168.10.x, with x being any number between 2 and 99
Subnet Mask	255.255.255.0
Gateway	192.168.10.1
DNS Server	192.168.10.1

Open your browser and enter the following into the address bar of your browser: http://cortexa. This will take you to the login page. If not, try using http://192.168.10.1 If this does not work please see the troubleshooting section in this Owners Guide.

Continued

CONFIGURING THE ROUTER

This section details how to configure the Router within the Cortexa to manage your network and gain access to the Internet through your Internet Service Provider (ISP). Your ISP may require the use of a Host Name and Domain Name. You will need this information from your ISP. If you do not have this information, please contact your ISP before proceeding. Document any changes from default by printing the page before saving, and making notes of passwords that are not displayed.

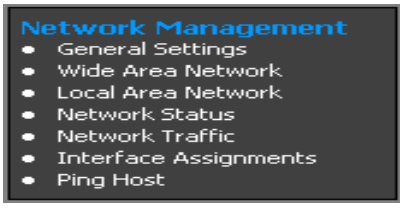


You should now be at this login page. Enter admin in the User Name field, and cortexa (the default password) in lowercase letters in the Password field. Optionally click on the box to remember this password for subsequent logins with this user name. Then click OK.

The Cortexa 7202 Home Page will appear. Click on Tools to go to the configuration page.

You will get a new login screen to gain access to the Cortexa 7202 Configuration Utility. Use the same User name and Password as above. You will now be in the Cortexa Configuration Utility. On the left of the screen each menu section will be highlighted in Blue with sub pages below. Find the Interfaces Section and Click on Status.

The Cortexa 7202 WAN Interface Status will appear at the top of the page.



WAN Interface	
Status	up
MAC Address	00:40:f4:8a:4d:bc
IP Address	24.153.224.196
Subnet Mask	255.255.255.192
Gateway	24.153.224.193
Media	100baseTX <full-duplex>
In/Out Packets	11510105/1326975 (1.11 GB/289.54 MB)

If the IP address has a valid address then you should be able to connect to the Internet. Open another browser window and try to log on to a site you don't normally visit, to avoid loading a cached page.

Continued

DHCP

If you are connecting through DHCP or a dynamic IP address from your ISP, perform these steps:

1. Select DHCP as the TYPE. **Type** DHCP
2. Click the Save button to save this setting.

STATIC IP

If you are connecting through a static or fixed IP address from your ISP, perform these steps:

1. Select Static IP as the TYPE
2. Enter the IP Address
3. Select the Subnet Mask
4. 4nter the Gateway
5. Enter the DNS in the 1, and/or 2 fields. You need to enter at least one DNS address
6. Click the Save button to save the settings

Static IP Configuration	
IP Address	24.153.134.11
Subnet Mask	255.255.255.248
Gateway	24.153.134.11

PPPoE

If you are using DSL and are connecting through PPPoE and if you normally enter a user name and password to access the Internet, perform these steps:

1. Select PPPoE as the TYPE
2. Enter the User Name provided by your ISP
3. Enter the Password provided by your ISP
4. Optionally enter the Service Name
5. Click the Save button to save the settings

PPPoE Configuration	
User Name	
Password	
Service name	Hint: this field can usually be left empty

PPTP

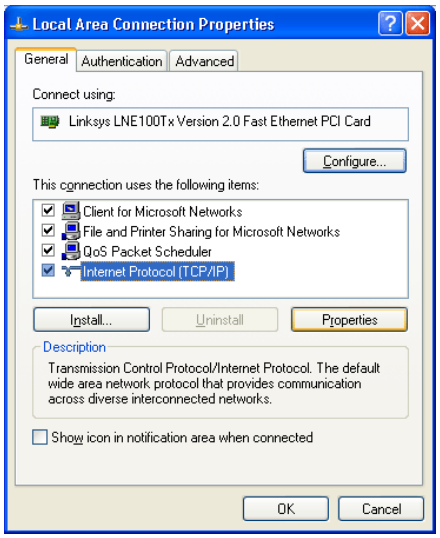
PPTP is a service used mainly in Europe. If you are using a PPTP connection, check with your ISP for the necessary configuration information.

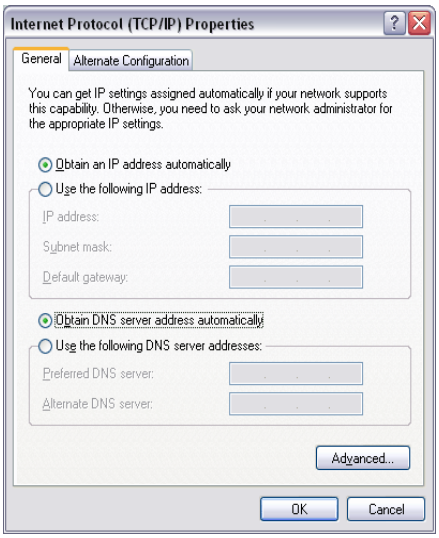
PPTP Configuration	
User Name	
Password	
Local IP Address	/ 31
Remote IP Address	

CONFIGURING YOUR PCS TO CONNECT TO THE CORTEXA 7202

Now that your router is configured, configure all PCs on the network to accept the IP addresses that the Cortexa 7202 will assign.

1. Click the start button, click Settings and open the Control Panel. From there, double-click the Network and Dial-up Connections icon. This will display the Network screen.
2. Right click on Local Area Connection icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed), then select Properties.
3. In the Configuration window, select the Internet Protocol (TCP/IP) and select Properties.
4. Select Obtain an IP address automatically.
5. Verify that Obtain DNS server address automatically is selected. Then click the OK buttons on this and subsequent screens to complete the PC configuration.





MAIN MENU

SYSTEM INFORMATION

The home page provides detailed system information. Here you see the resources that are being used, the status of the Cortexa hardware, and weather data that is being received.

System Information	
Serial Number	00:40:63:df:df:4c
Version	V3.07 Beta,Build 1620 built on Thu Apr 6 11:07:17 2006
Platform	Cortexa 72XX
Uptime	03:42
Last config change	Wed Apr 5 10:58:17 CDT 2006
CPU usage	14% view graph
Memory usage	60%
Sunrise	07:12:23 AM
Sunset	07:49:50 PM

2006-4-6 14:58:47	CURRENT	MIN/MAX
Temperature (°F)	84.1	72.1 / 84.1
Humidity(%)	47	47 / 73
Wind (mph)	5.0	26.0
Wind Gust (mph)	10.0	0.0/26.0
Wind Direction °	SW	227
Pressure ("Hg)	29.21	29.21 / 29.27
Day Average Wind Speed (mph)	7.72	-
Heat Index (°F)	84.60	-
Wind Chill (°F)	84.10	-
Dew Point(°F)	61.70	-
Day Rain Fall (in))	0.00	-

Five Day Forecast

Thursday	Friday	Saturday	Sunday	Monday
Hi: 90°	Hi: 88°	Hi: 76°	Hi: 82°	Hi: 83°
Lo: 58°	Lo: 52°	Lo: 49°	Lo: 54°	Lo: 59°
Isolated T-Storms	Sunny	Sunny	Sunny	Sunny

Warnings and Watches

None

There are currently no watches, warnings, or advisories in effect.

CHANGE PASSWORD

The password section allows the current user to change passwords. If logged in as admin, this will change the admin password.

OWNER INFORMATION

This should be setup by the installer to help the end user know who installed the system and who to contact if they need help. This information can only be used changed by the administrator.

ADMINISTRATION

The Administration section allows you to configure who has access to the Cortexa, and what permissions are allowed. This section is also used to update firmware, and to backup and restore your settings.

USER MAINTENANCE

Add a list of users that are allowed to access the Cortexa. This gives better security control without having to give out the master password. This also provides the ability to determine which, if any, of the configuration functions within the Cortexa each user may access.

BACKUP / RESTORE

This section will allow you to back up and restore all of your settings. You should backup your data after you have initially configured the Cortexa, and then at frequent intervals thereafter.

SOFTWARE UPDATES

In our drive to continually improve this product, frequent software updates will be released. All software updates are free to existing users, and easy to install. We want all users to enjoy the latest software and the functionality and reliability it provides. First check to see if new software is available by clicking the Check Now button. If a later release of firmware is available, simply click the Update Now button. The new software will now be downloaded to your Cortexa. This will take approximately one minute. You will then be prompted to reboot the Cortexa. Upon reboot, the new software will be installed and running.

REBOOT SYSTEM

Select reboot system and click YES. A reboot will take approximately one minute.

FACTORY DEFAULTS

If you select to restore the factory defaults settings, click the YES button. You will clear all current Cortexa settings and restore factory default settings.

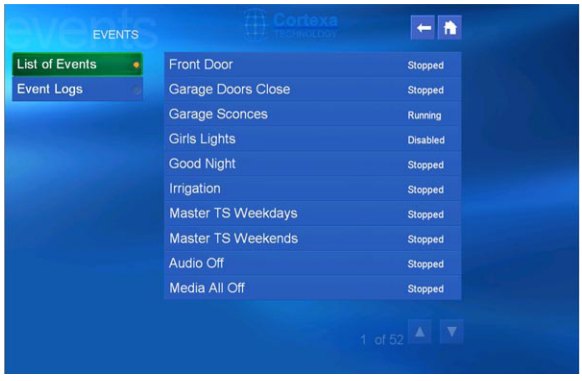
HOME MANAGEMENT

EVENT MANAGER

Events allow the automation of all sub-systems and devices throughout the home, in a completely integrated way. This section will cover the key parameters involved in event writing, followed by some examples to illustrate their uses.

Writing events with the Cortexa system does not require the learning of a programming language unlike many systems. At every step, the system presents the user with valid choices from drop-down menus. Do not think this is complicated, or beyond you. Many of our customers start off saying they will not write their own events, then actually do when they see how simple it is. Events may be written and executed from anywhere you have access to your Cortexa.

EVENT USER INTERFACE



On the right is the Event page from the Cortexa User Interface. From here, you can view a list of all events within the system, and run an event by pressing the play button. You can also view the status of an event, enable an event, or disable an event. For example, you may have a morning event that automatically turns on music throughout the home at 6.30am every weekday. On vacation days you may not want the event to run, so simply pressing disable will stop the event from running until it is re-enabled.

NAMES, TRIGGERS, CASES AND ACTIONS

These are the four things to consider in event writing. Here's what they are and how they are used:

NAME

Each event must have a unique name. Be sure to name events with a name that indicates what they do. For example, an event run before going to bed might be called "Goodnight". After a while you will have many events in your system.

TRIGGER

Events may or may not have a trigger. The trigger is what will start the event running. There are many possible triggers; time, sunrise/sunset, weather condition and so on. For example, a lighting scene may be triggered by sunset. Most events have triggers. Without a trigger, an event will only run when manually initiated. There are events where you will want this to be the case. An example might be audio events. Other than perhaps turning on audio when you wake in the morning, for the most part it will be a spontaneous decision to listen to music throughout the home. But when that time comes, just start the event and the music can be playing in every room, from the same or different sources, at the desired volume in each room.

CASE

Events may or may not make use of case statements. A case is a condition that will be tested, then dependent on the outcome of the condition, the action will or will not execute. A good example is with irrigation events. You have an event that turns on your sprinkler zones, however you don't want to water your yard if the wind is blowing at 25 mph just when you are ready to water. The condition of the case would then be to check wind speed. We will look at this specific example later in this section.

ACTION

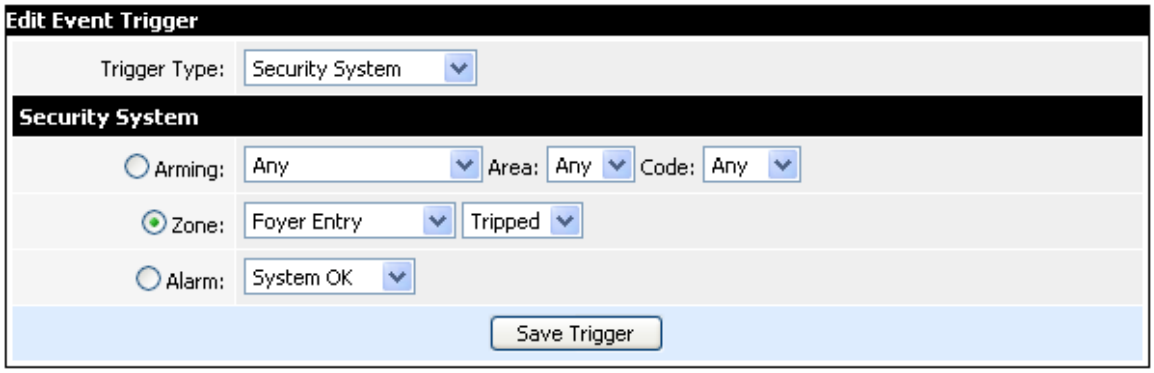
All events will have at least one action statement. Without an action statement an event would not perform any function. Action statements will typically involve one or more devices. For example, turn light(s) on, set thermostat temperature, set audio source, record video from a camera. There are also situations, such as having the system send you an email, where no device is involved, however this is still an action.

EXAMPLES OF EVENTS

Here we will look at four actual events to help you see how the above parameters work together. In each case, we will explain what the event does, followed by screen shots and some brief explanations of what each screen is doing. To create an event, simply go to the Event Manager within Home Management, enter the name of the event in the Event Description field, and click Add New Event. You will then be able to configure the event trigger, case and actions. Case and Actions are accessed through the "Edit Macro" button.

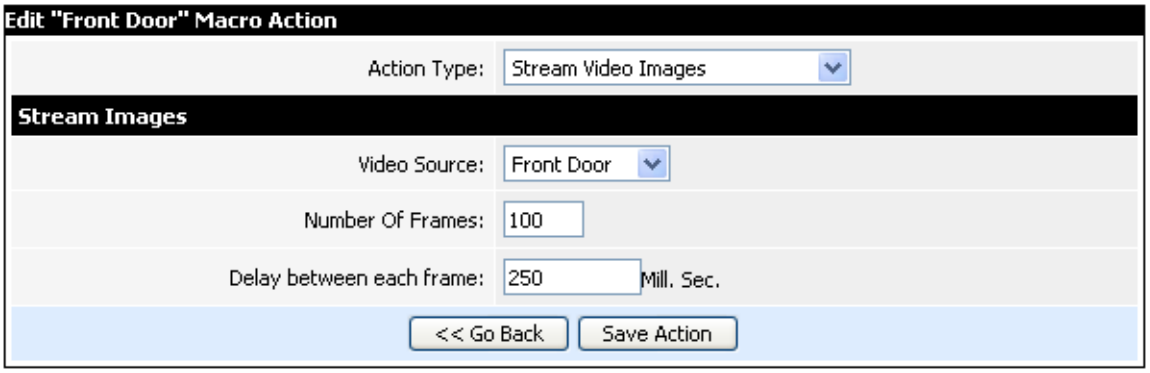
FRONT DOOR ARCHIVE

This event records video from a camera every time the front door is opened. Below is the trigger. This is from the Security System, and specifically the zone called Foyer Entry and when the zone is tripped, i.e. the door is opened. Every time the door this opened, the trigger will initiate this event.

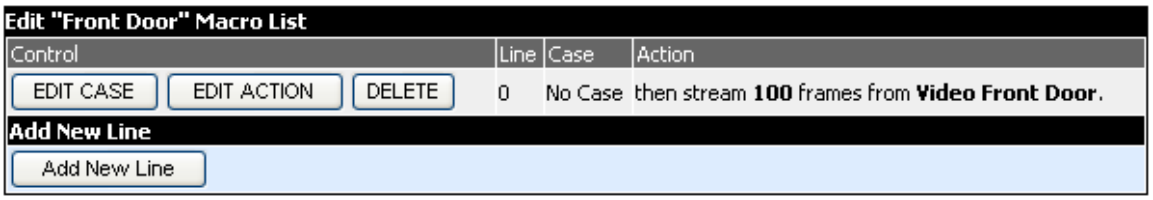


Having established the trigger, we then think about whether we want to have a case condition. In this situation, the answer is no. Every time the door opens, we want this to execute, so there is no case involved. We then move to Action. This is where we tell the system what we want the event to do, having been triggered.

On the next page, you will see that in this case, our action is "Stream Video Images", i.e. start the camera recording. The system then asks which video source. We select Front Door (the name of the camera over the front door). The system then gives us the option to select the number of frames and the frame rate. These will obviously determine the quality and length of the recording. Here we have selected 100 frames at 250 milli second (one quarter of a second) intervals. This will give us 25 seconds of good quality video.



The event is now complete and looks simply like this.

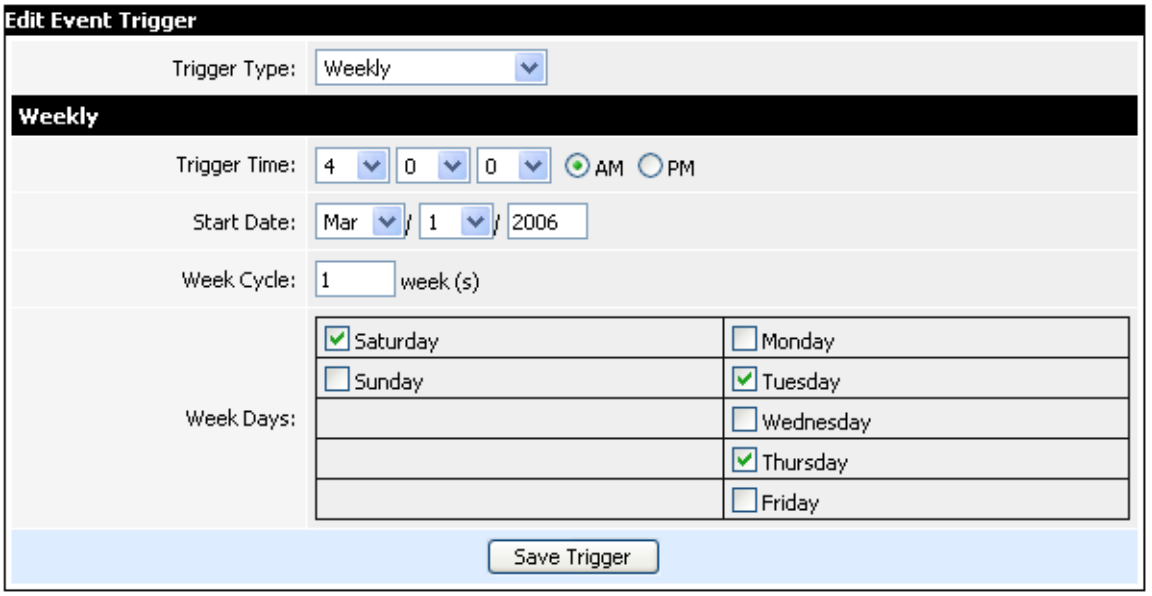


This is not a very complicated event, however we hope you can see how simple and fast it is to create, and not one line of programming code involved! When you become proficient with the system, events like this can be created in just a few seconds.

IRRIGATION

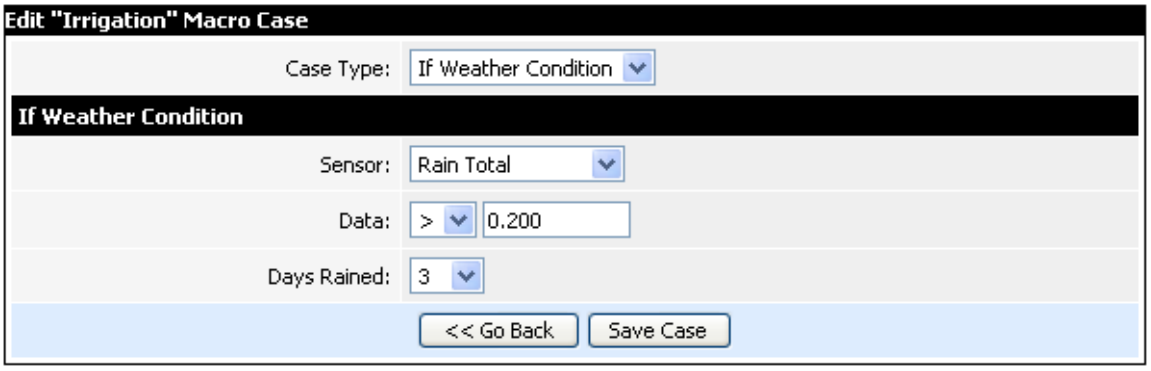
This event turns on two zones of irrigation, however we care about the environment (and our water bill), so have added some intelligence in the form of two cases.

Firstly, the trigger. This is time based; specifically we want to irrigate three days per week. The trigger type is Weekly, and as you can see we have entered our desired parameters in terms of which days and what time we would like to start watering.

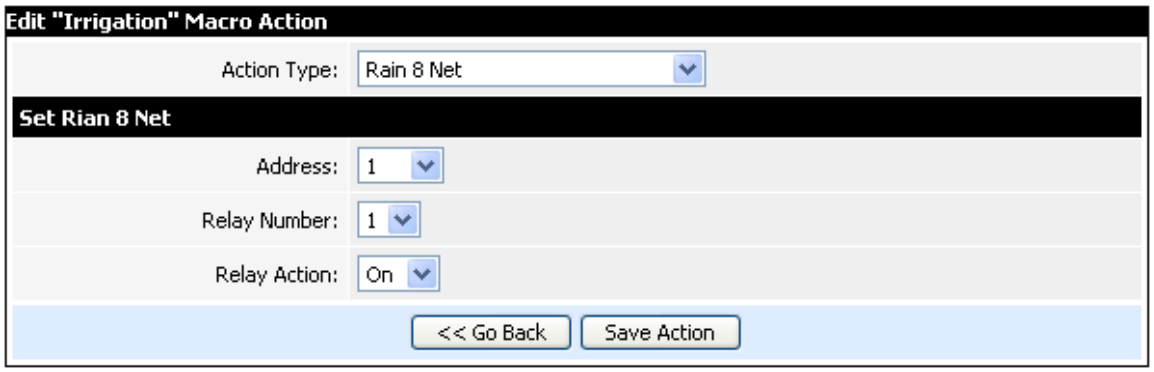


We now click Edit Case. In this situation, our case is a Weather Condition. That condition is based on Rain Fall. Since the Cortexa is collecting local weather data every fifteen seconds, not only does it know current weather conditions, it is also able to calculate historical data. We decided our criteria to be based on 0.2" over the last three days.

We also added another case condition based on current wind speed. You will see that when we look at the finished event.



Having established our trigger and cases, we are ready for action. The action is to water the yard. The Action type is "Rain 8 Net", the name of our Irrigation system. The Irrigation module comes in 8 zone increments, each one having a unique address. The relay number then corresponds to the irrigation zone. Here we are turning on zone 1, i.e. Address 1, Relay 1. As an example, zone 9 would be Address 2, Relay 1.



The following screenshot is the completed event. After each case statement, we selected End Macro. End macro immediately halts the entire event, i.e. none of the actions commands are executed. Obviously this is what we want here. If first condition is true, i.e. the wind is blowing at more that 15 mph, we do not want to water the yard, no matter what else is true or false.

The command "Sleep For" is used to let the sprinkler zone run. So for zone 1, we open it, then the event goes to "sleep" for 10 minutes. After exactly 10 minutes, the event "wakes up" and turns off that sprinkler zone.

Edit "Irrigation" Macro List

Control					Line	Case	Action
EDIT CASE	EDIT ACTION	DELETE	DOWN		0	If Wind Speed is > **15.000**	then end macro.
EDIT CASE	EDIT ACTION	DELETE	UP	DOWN	1	If Rain Total is > **0.200** for 3 day(s)	then end macro.
EDIT CASE	EDIT ACTION	DELETE	UP	DOWN	2	No Case	Turn Rain 8 Net **A:1 R:1 ON**.
EDIT CASE	EDIT ACTION	DELETE	UP	DOWN	3	No Case	then sleep for **10**minute(s) .
EDIT CASE	EDIT ACTION	DELETE	UP	DOWN	4	No Case	Turn Rain 8 Net **A:1 R:1 OFF**.
EDIT CASE	EDIT ACTION	DELETE	UP	DOWN	5	No Case	Turn Rain 8 Net **A:1 R:2 ON**.
EDIT CASE	EDIT ACTION	DELETE	UP	DOWN	6	No Case	then sleep for **6**minute(s) .
EDIT CASE	EDIT ACTION	DELETE	UP		7	No Case	Turn Rain 8 Net **A:1 R:2 OFF**.

Add New Line

Add New Line

SUNSET LIGHTING

This is a very simple event which we will use to highlight one of very useful features of Cortexa event writing; the use of flags. Flags can be used within cases to add some form of condition or additional intelligence to the event.

The event simply turns on our desired lights, to their desired intensity level, at sunset each day.

Here we are using sunset as our trigger. We also have the option to set variances from both sunrise and sunset. We have decided that we'd like the lights to come on before sunset as at sunset it is already a little dark in the house. We can set variances + or – and with hours, minutes and seconds. In this case we are telling the event to launch 10 minutes before sunset.

Edit Event Trigger

Trigger Type: SunRise/SunSet

Sunrise/Sunset

☐ Sun Rise:	-	0	0	0
☑ Sun Set:	-	0	10	0

Save Trigger

Continued

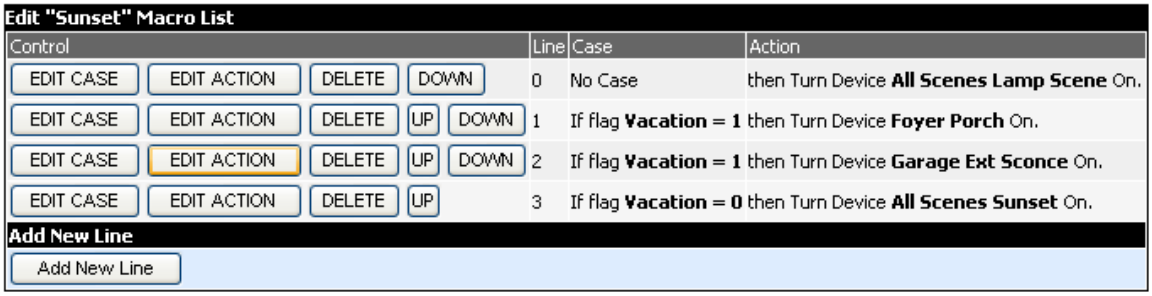
Our flag is called “Vacation”. Flags are setup up in the Flag Manager, again within Home Management. Our vacation flag, as you might imagine, indicates whether we are home, or on vacation. We would like a different lighting scenario to take place when we are on vacation, i.e. less lights to come and not be wasteful of energy.

Flags have a value, which can set in the Flag Manager. They can also be modified by an action in an event. In this case, we have the flag set up such that when we go on vacation its value is 1, otherwise it is 0.

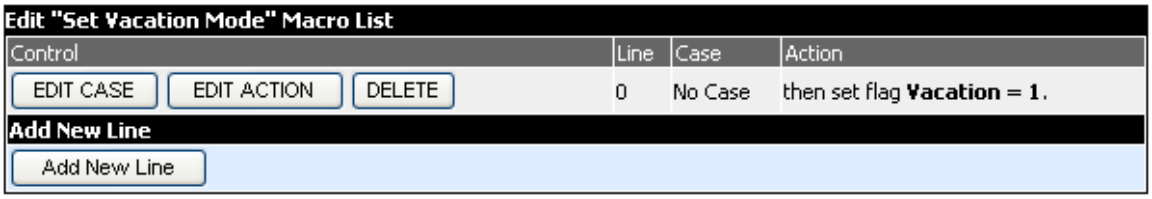
So let’s look at the event. Both “Lamp Scenes” and “Sunset” are pre-defined lighting scenes that have already been set up. Line 0 in this event will always run, i.e. whether we are on vacation or not, we want the lamps to come on.

Lines 1& 2 will run if we are on vacation (because the vacation flag will be set to 1), but not if we are not.

Line 3 is the opposite of 1&2. It runs when we are home. This turns on lights throughout the home, just as we want, but only if we are home!

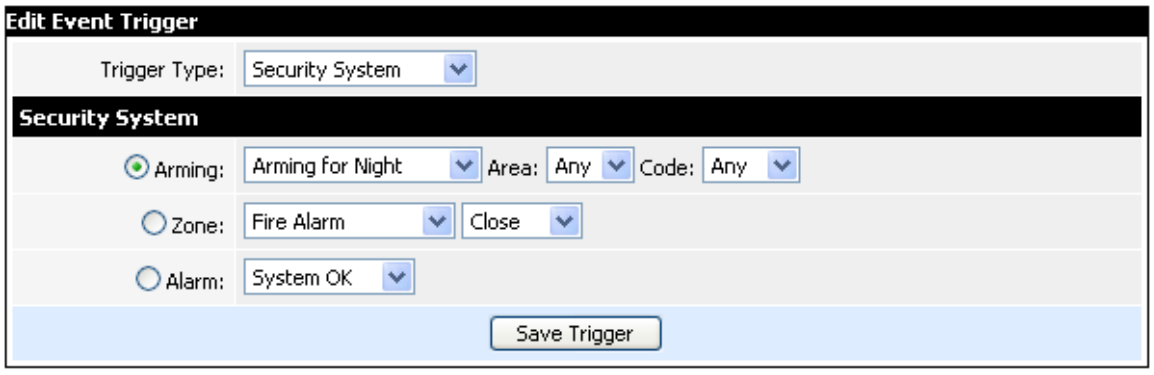


To set the vacation flag, use a simple action statement as below.

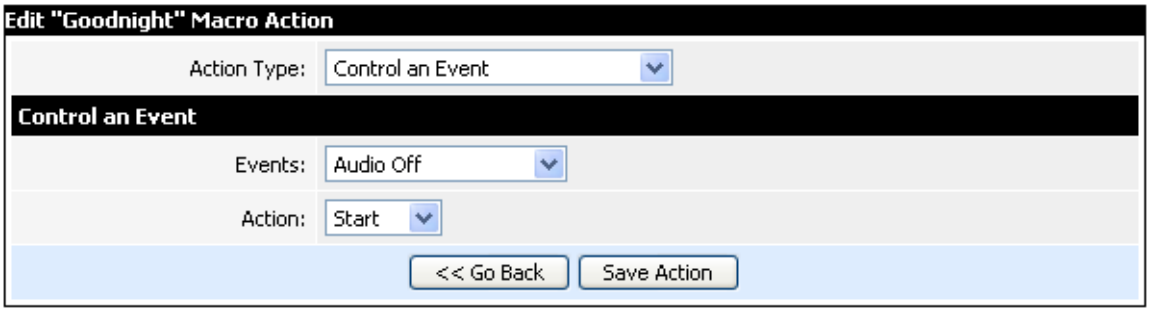


GOODNIGHT

This event runs last thing at night. We will use it to highlight another nice feature; the ability to run an event from within another event. The trigger is the arming of the Security System with any user code. If you have multiple codes, you can write events specific to the code used to arm, or disarm, the system.

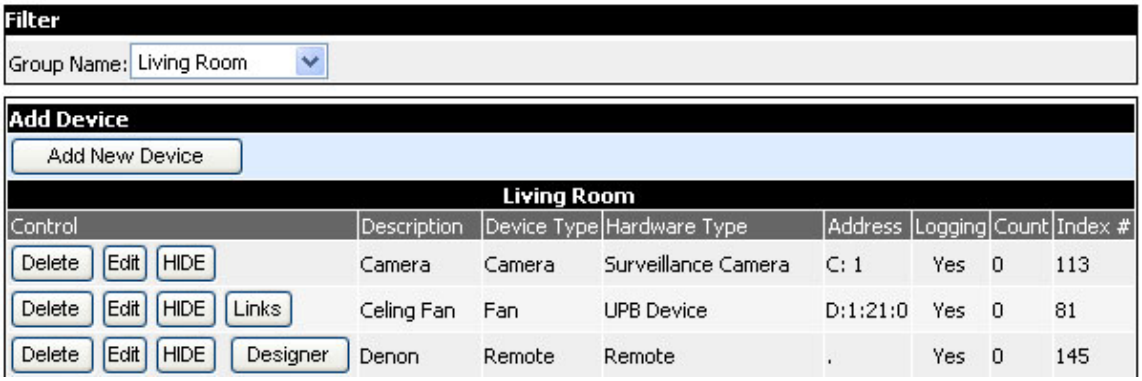


We have an existing event called "Audio Off" that turns off all audio throughout the home. We'd like to do that as part of this event. Instead of having to write the actions for that event again, we simply select "Control an Event". The system then prompts us for the name of the event from a drop-down menu with the names of all of our events. We select "Audio Off", then tell the system to start the event.



The entire event is below. After turning off our audio, we send commands to a TV, Receiver and DVR to turn off. We then run another event that we have previously written, "Garage Doors Close". This event checks to see if all doors are closed and closes any that are open. We then adjust three thermostats for comfortable sleeping temperatures, and finally run two lighting actions to configure the lights how we like them during the night.

DEVICE MANAGER



- Control: Enables selection of the module you would like to delete or edit
- Description: The description you give the device
- Device Type: The type of device that is being controlled
- Hardware Type: The type of hardware used
- Address: The current address of the hardware
- Logging: It will log the action to the log file, when an action from the module is received
- Count: The number of times the device has been turned on
- Index #: The database index number

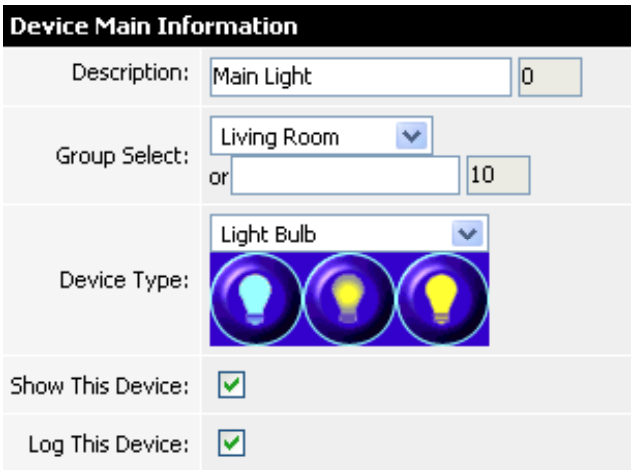
Each device added is associated with an area (room). In the user interface under Areas, you will then see and have control of, each device within that specific room.

It is possible to associate one device with multiple areas. This is useful for thermostats, for example, where one thermostat may control multiple rooms.

EDIT DEVICE PAGE

Once you click add new device, or edit device, you will be taken to the Edit Device Page. If this is a new device, you will need to select the device type first.

DEVICE MAIN INFORMATION



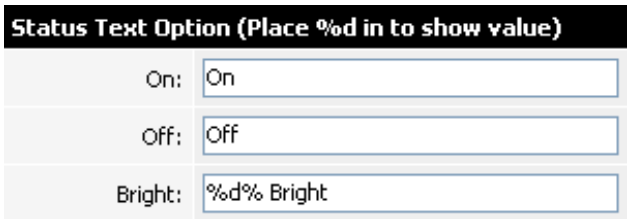
Here you will enter information about the device:

- **Description**: This is what you wish the device to be named. You should keep it less then ten characters otherwise the description will be truncated on the User Interface.
- **Group Select**: This is how you will group the device in an Area. You may select an existing group, or create a new group. You should also keep this less then ten characters.
- **Device Type**: This allows you to associate an icon with what the device is controlling. This is also how devices are grouped in the User Interface.
- **Show This Device**: If selected, the device will be displayed in the User Interface.
- **Log This Device**: If selected, the device will be logged every time it changes status. You may wish to turn this option off for high traffic devices, e.g. motion detectors, so that the log files will not get full for just one device.

DEVICE ADDRESS INFORMATION

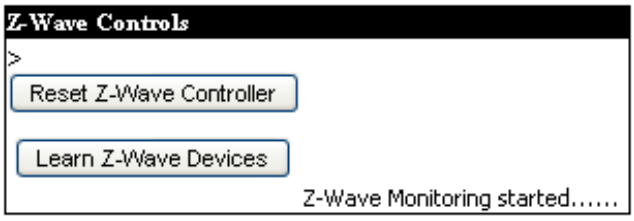
This section changes depending on the device type. Each type has a unique way of being addressed. Please refer to the device manual on configuring addresses.

DEVICE STATUS TEXT



The Status Text option allows you to modify the way the status is shown in the control and log screens. Depending on the device type, some of these fields may not be here.

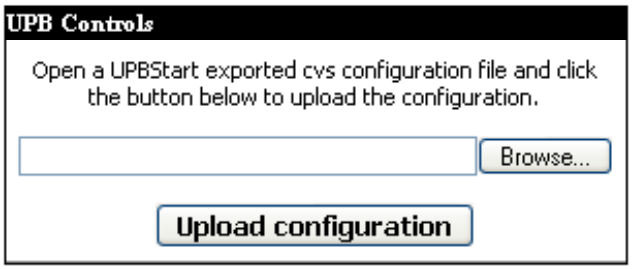
Z-WAVE



If you are using Z-Wave, you will have to learn the new device into your hand held remote, and then copy the remote to the Cortexa. If a device is already in the list, the learning process will not overwrite it.

You should reset the controller if this is the first time you have used the Z-Wave interface module. If you reset the Z-Wave Controller, all of your existing devices will be deleted.

UPB



To setup UPB, you will need to download the UPB UPStart utility from PCS at http://www.pcslighting.com/.

Once you have setup your lights and scenes using the UPB UPStart utility, you will then export the devices in the utility, and import the file into the Cortexa.

INSTEON

Install devices as per manufacturer's instructions. The process to configure devices in the Cortexa is called enrollment and is performed as follows;

Hold the "set" button on the Insteon Powerlink module for 10 seconds, then put the Insteon device to be configured in "setup" mode. Refer to the manufacturer instructions on how to do this.

The device will now appear in the Cortexa Device Insteon Group. Go to the Edit Devices screen and move the device to the Area in which it is installed. The device is now configured and ready to be controlled and written into events. Refer to the Cortexa Insteon Installation Guide for more detailed information.

LUTRON RADIO RA

Install devices per manufacturers instructions. Having configured the devices and scenes within the Lutron system, they now need to be entered in the Cortexa. Carefully note which Lutron Radio RA switch number corresponds to the physical location of each device.

Similarly, for scenes that have been created in Lutron, note all scene numbers for input to the Cortexa.

To configure the device into the Cortexa, go to the Add Devices screen. Select Radio RA and enter the address and area data. In order to configure a scene, enter that scene number as a Phantom button.

LUTRON HOMEWORKS

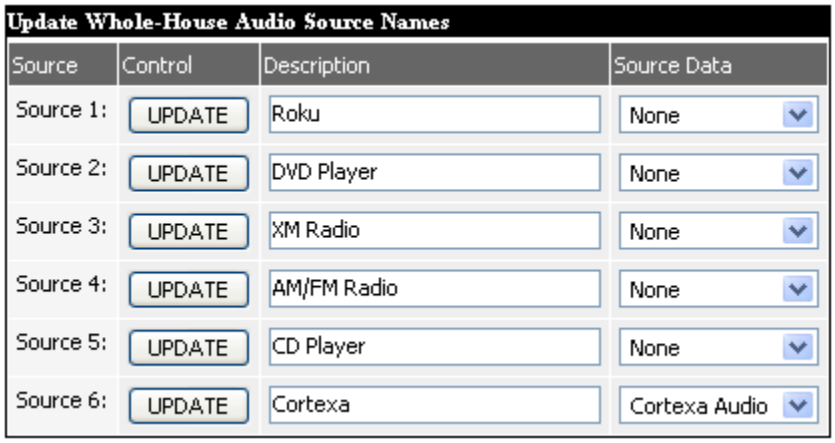
Install devices as per manufacturers instructions. Having configured the devices and scenes within the Lutron system, they now need to be entered in the Cortexa. Carefully note which Lutron Homeworks switch number corresponds to the physical location of each device.

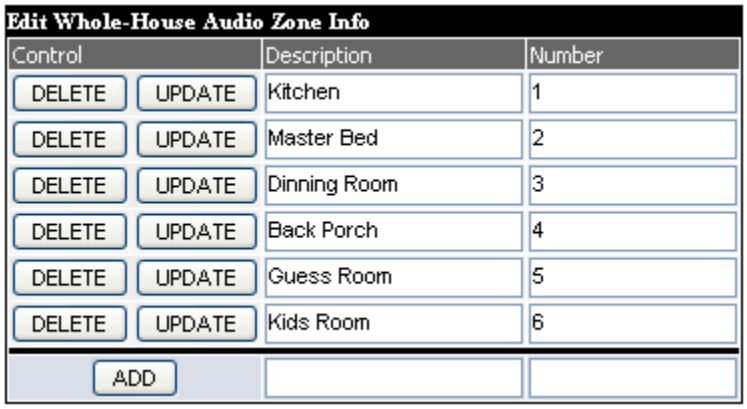
Similarly, for scenes that have been created in Lutron, note all scene numbers for input to the Cortexa.

To configure the device into the Cortexa, go to the Add Devices screen. Select Homeworks and enter the address and area data. In order to configure a scene, enter that scene number as a Phantom button.

NUVO AUDIO DISTRIBUTION

The Cortexa has a built-in interface to the NuVo Technologies Essentia and Concerto Audio Distribution systems. In order to customize your own zones and sources, go to the Device Drivers page, select which system you have, then click on Advanced. You will then be able to enter sources and zones, exactly as you desire. When using the touch screen or web browser interface, you will then be able to fully control all audio sources and zones.





DEVICE MANAGER (IR)

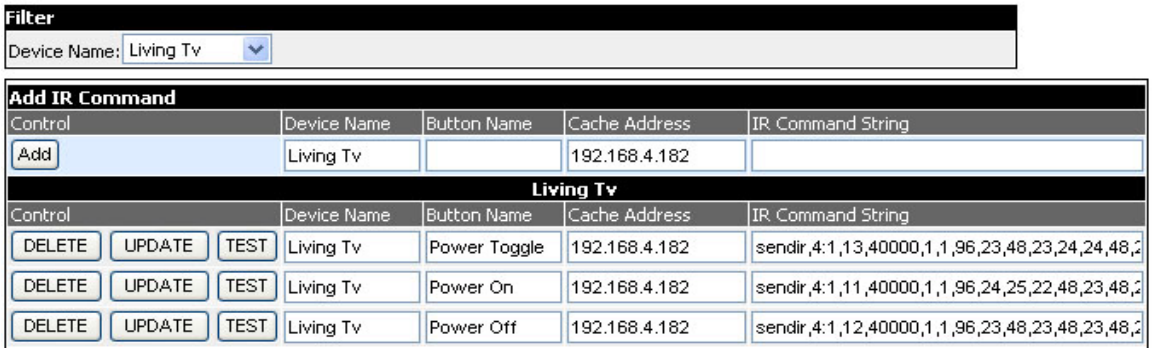
This section allows you to create a list of IR Commands to control your IR devices. If you have not already done so, connect your Global Cache module to a network switch and configure it to a specific IP address. Details on how to set the IP can be found at www.globalcache.com.

IR commands are learned using a Global Cache GC-IRL IR Learner. The IR learner is first connected to a PC through a serial interface. Then go to www.globalcache.com and download the learner application to your PC. Launch the application, making sure you see "connected" in the bottom bar of the application window. This indicates the Learner is communicating with the PC serial port, and is ready to learn IR strings.

Now point your remote at the Learner and press the desired button. You will see the IR string appear on the screen. This string is automatically in the clipboard. From there, go to the IR screen below and simply paste the string into the field. Make sure you name the device to which the string relates and the specific button name. The more descriptive you make these names; the easier it will be when you are recalling them to build a customized remote control.

Building a remote control customized to your needs is easy with the Cortexa's Remote Control Designer. First go to Add Devices, add a Remote and associate it with the Area of your choice. Then go the Edit Devices, and beside the entry for that remote you will see a Designer button. This takes you into an application that let's you set up your remote. Note there are two sizes of remote. For touch screens and web browsers, use the large remote. The small remote will be used in the future for PDA and webpad devices.

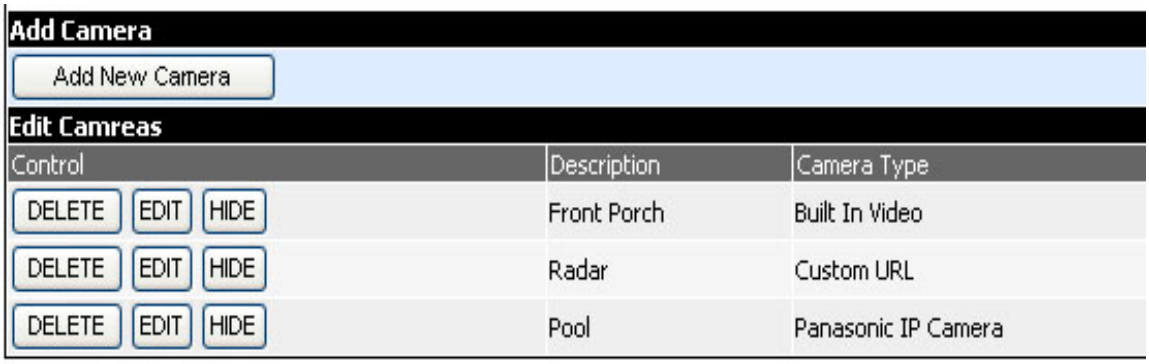
The Designer is highly intuitive and allows you to add buttons, either custom labeled or fixed such as Power, then drag and drop them to the desired position on the screen. You can program any button to associate with any IR string you have learned, as above. Also, not only can the remote activate an IR command string, it can also initiate any Cortexa event. For example, in a home theatre setting, you might have an event that turns on a DVD player, sets the channel on a receiver, dims lights and adjusts thermostat settings. This event could then be activated by a "DVD" button on the custom remote. As you spend time creating remotes, we think you will find this functionality easy to use, flexible and powerful. Enjoy!



- Control: Enables selection of module you would like to delete or edit
- Device Name: The name of the device to be controlled
- Button Name: The name of the button to be controlled
- Address: The IP Address of the global cache device where the commands are going to be sent
- IR Command String: The string that is created by the Global Cache IR Learner

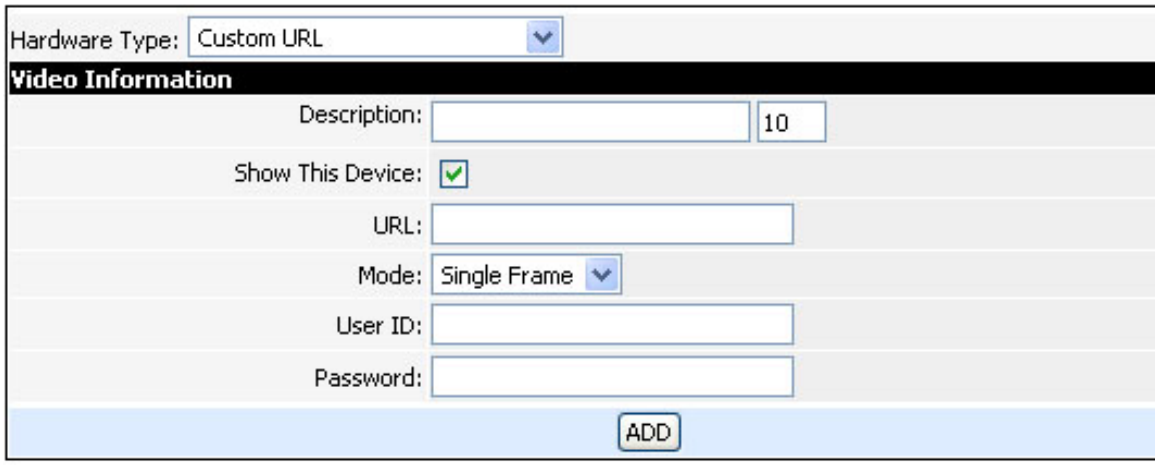
CAMERA MANAGER

The edit video list page allows you to manage the video source.



- **Control:** Allows the video source information to be deleted, edit, hidden, or shown.
- **Description:** A description of the video source.
- **Camera Type:** The template used to get camera images.

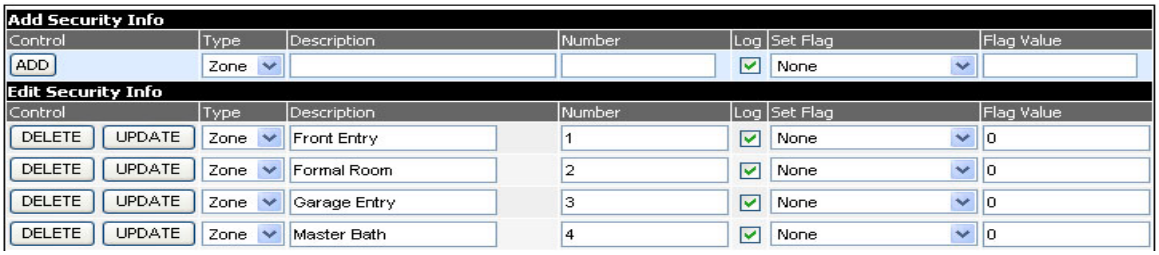
EDIT CAMERA



- **Hardware Type:** This tells the Cortexa how to get this image.
- **Description:** A description for the video source.
- **Show This Device:** This allows you to hide the camera from the User Interface screens.
- **Mode:** Still images will take a single shot, and require a screen refresh to view a new image, while Streaming will continually stream camera images.
- **User ID:** The user ID for the image source if required.
- **Password:** The password for the image source if required.

To create a new entry, you can use either the wizard for cameras that we support, or manually enter a source of your own.

SECURITY MANAGER



The security system zone information from your security system is entered here:

- **Type:** The type of zone information
- **Description:** The name of the zone
- **Number:** What zone number this is associated with
- **Log:** Log this zone on activity. You may wish to not log motion sensors
- **Set Flag:** This is useful for events. For example, you can keep setting a flag to a value as long as the activity is happening so that a light might stay on
- **Flag Value:** If setting a flag, this is the desired value to set the flag

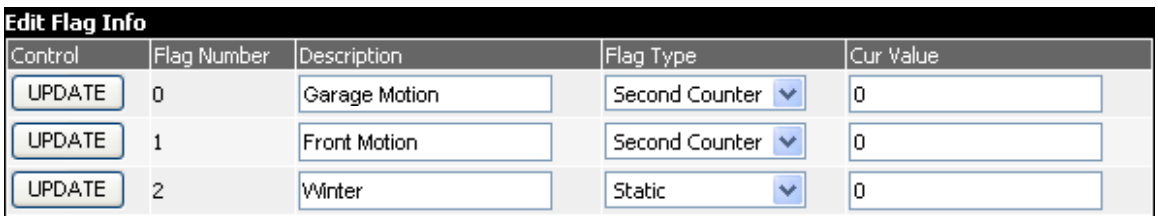
HAI SECURITY TOOLS

If you have a HAI Omni security system, you can upload and download zone information automatically between HAI Omni and the Cortexa.

FLAG MANAGER

Flags can be useful with events. The Cortexa comes with 128 usable flags. There are two types of flags; Static, and Second Counter. The Static flag is useful for status on something that will have only two states, e.g. vacation mode. The Second Counter is useful for keeping lights on for specific periods of time. The Second Counter is a down counter only.

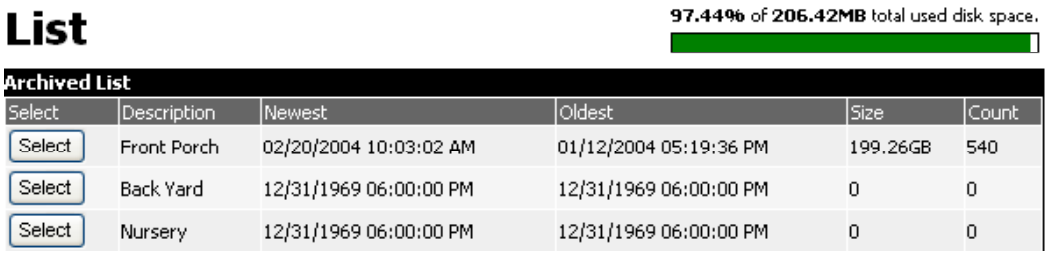
Static flags are stored in flash memory, so if power fails, when the Cortexa comes back up it will continue where it left off. Second Counters are not stored in flash, so when the Cortexa comes backup, the current value will be set to 0. Once the down counter reaches 0, the counter will stop.



VIDEO ARCHIVE

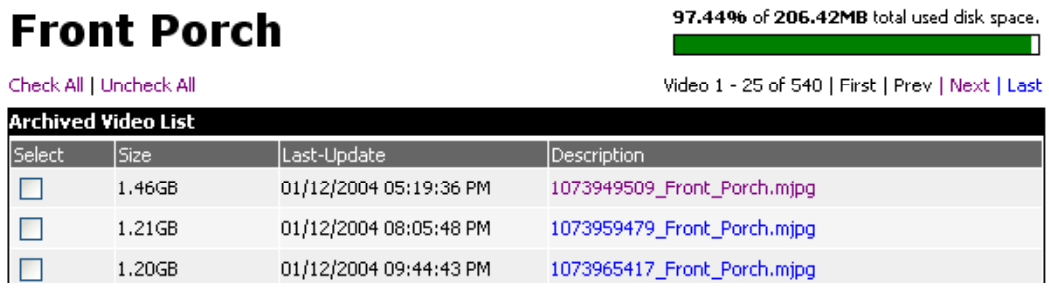
This section allows you to view and manage the archived video stored on the built in flash memory.

The bar graph (top right) shows how much disk space is left on the built in flash memory.



- **Select:** Allows you to select the camera to view
- **Description:** The name of the camera gives in the edit video list page
- **Newest:** The time and date of the newest file captured
- **Oldest:** The time and date of the oldest file captured
- **Size:** The amount of flash that the archive for the specific camera is using
- **Count:** The number of files stored for the specific camera

Once a camera is selected, you will see the list of archived files. You will be able to view 25 at a time.

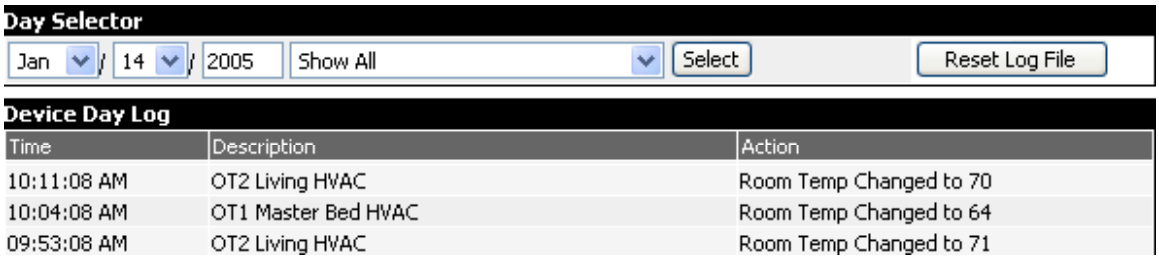


- **Select:** Select the images to be deleted.
- **Size:** The size of the image files.
- **Last-Update:** The time and date the last time the archived images were updated.
- **Description:** The name of the video source with a time stamp in front of the name.

REPORTING

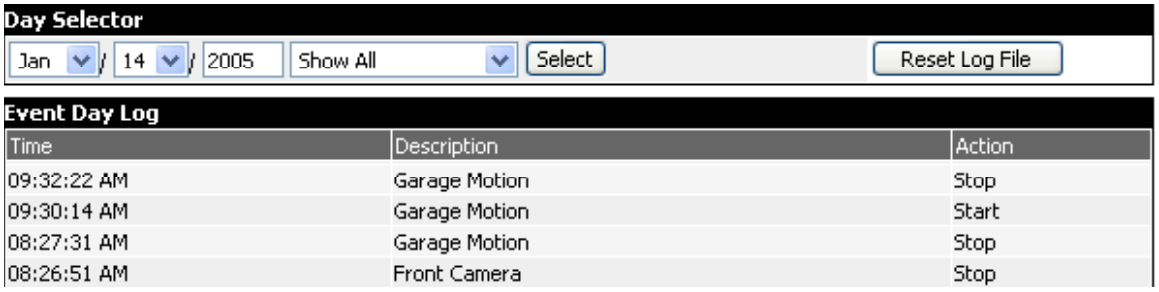
DEVICE LOGS

The device logs display all device status changes. The day selector may be used to go back to a specific date to review the activity.



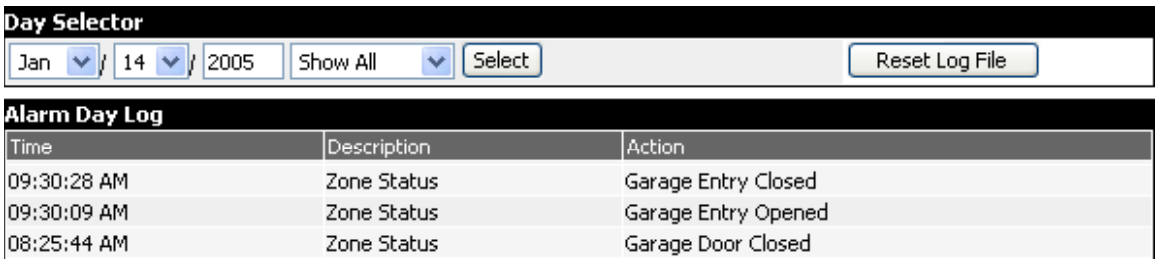
EVENT LOGS

The event logs display all event activity and status changes. Again the day selector may be used to go back to a specific date to review your activity.



SECURITY LOGS

The alarm logs display all alarm status changes. Again the day selector may be used to go back to a specific date to review your activity. As previously mentioned, you may want to disable logging of high activity devices such as motion detectors. This is done in the Security section by un-checking the Log Device box.



SYSTEM LOGS

The system log is a list of warnings, and errors from the internal operating system. If a problem arises, this is the most logical place to start trouble-shooting.

Last 100 system log entries	
Aug 11 10:48:12	/kernel: Waiting (max 60 seconds) for system process `syncer' to stop...stopped
Aug 11 10:48:12	/kernel:
Aug 11 10:48:12	/kernel: syncing disks...
Aug 11 10:48:12	/kernel: done

CORTEXA LOGS

The Cortexa log will display any errors or warnings and errors coming from the home automation software.

Last 200 Cortexa service log entries	
Jan 14 09:07:17	HAIOMNID: Polling Started.
Jan 14 09:07:16	HAIOMNI: Logged into successfully
Jan 14 09:07:11	HAIOMNI: Trying to disconnect...0

FIREWALL LOGS

The firewall logs show packets that where blocked by the firewall. Activity as below is normal.

Last 100 firewall log entries	
Aug 11 10:48:19	ipmon[80]: 10:48:16.828196 sis0 @0:13 B 192.168.4.50,4858 -> 24.153.142.234,143 PR tcp len 20 51 -AP IN
Aug 11 10:48:22	ipmon[80]: 10:48:21.996776 sis1 @0:13 B 216.136.233.153,25 -> 24.153.134.38,13629 PR tcp len 20 174 -AP IN

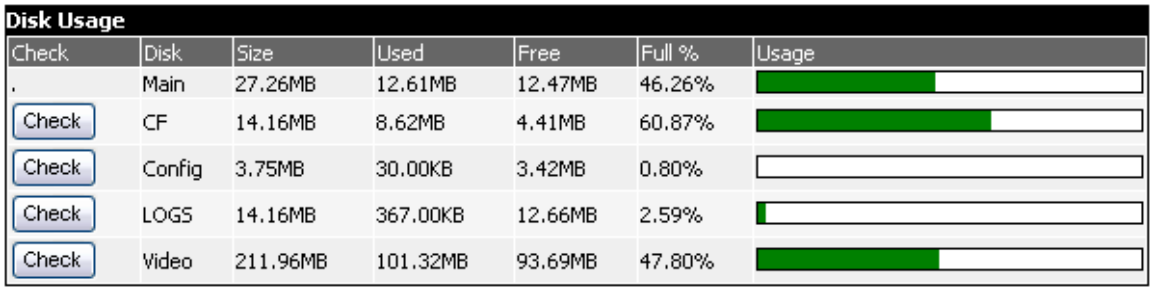
DHCP LOGS

The DHCP log shows the DHCP connections that are being requested by LAN clients.

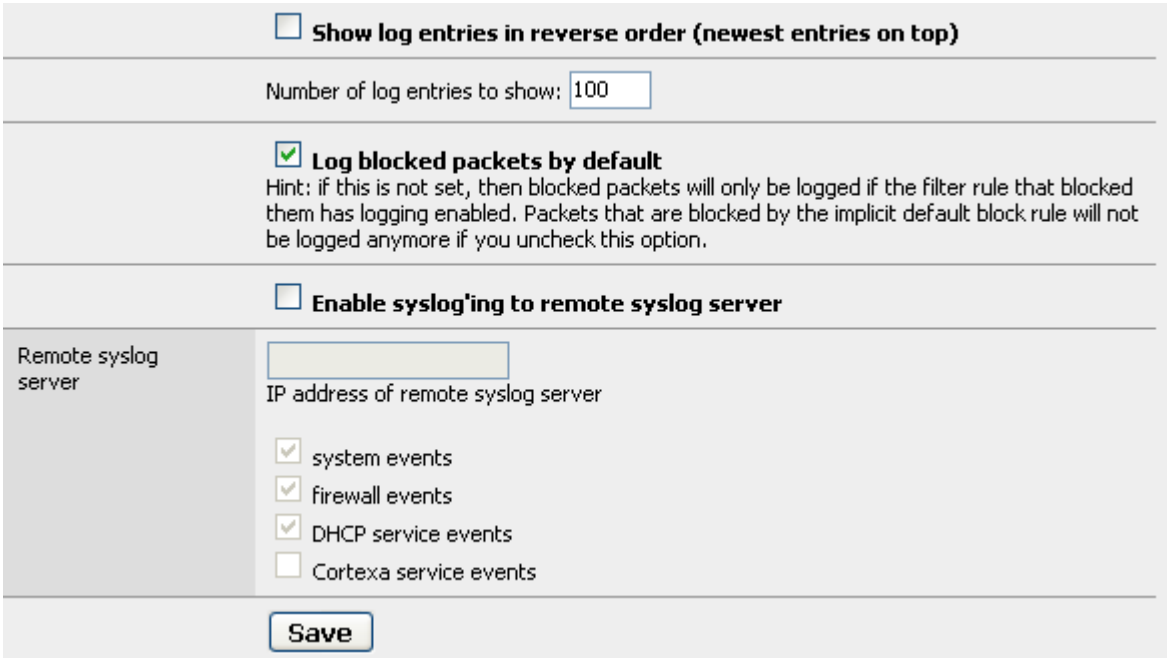
Last 100 system log entries	
Aug 11 10:48:15	dhcpd: Internet Software Consortium DHCP Server V3.0.1rc11
Aug 11 10:48:15	dhcpd: Copyright 1995-2003 Internet Software Consortium.
Aug 11 10:48:15	dhcpd: All rights reserved.

STORAGE STATUS

Shows the status of memory storage within the Cortexa. Memory is split into several partitions to keep write conflicts down to a minimum. Most of the time the Cortexa does not write to memory, so it is in read only mode. If logging information is being written to the log partition, the Cortexa will only unlock the log partition to perform this operation, then locks the partition back. This makes it safe to turn the Cortexa off without telling it to turn off. If a power outage occurs, memory integrity should not be compromised.



REPORTING SETTINGS



SETUP OPTIONS

SUB-SYSTEM SETUP

Sub-Systems

Sub-System	Com Port	Baud Rate	Device Type	Extra
X10 PowerLinc	Disabled	4800	NA	NA
Insteon	Com 7	9600	NA	Advanced
UPB	Com 5	4800	NA	NA
Z-Wave	Disabled	115200	NA	NA
HomeWorks	Disabled	115200	NA	NA
Radio RA	Com 2	115200	NA	NA
Vantage	Disabled	57600	NA	NA
Serial Relay (Bank 1)	Disabled	9600	8 Relays	NA
Serial Relay (Bank 2)	Disabled	9600	16 Relays	NA
Serial Relay (Bank 3)	Disabled	9600	8 Relays	NA
Serial Relay (Bank 4)	Disabled	9600	8 Relays	NA
Ascii Data (Bank 1)	Disabled	115200	NA	NA
Ascii Data (Bank 2)	Disabled	115200	NA	NA
Ascii Data (Bank 3)	Disabled	115200	NA	NA
Ascii Data (Bank 4)	Disabled	115200	NA	NA
Rain 8 Net	Com 3	4800	NA	NA
Security	Com 1	9600	HAI Omni Pro II	HAI Password: ••••
HAI Thermostat (Cortexa)	Disabled	600	NA	NA
Whole House Audio	Com 6	9600	NuVo Concerto	Advanced
Weather Station	Disabled	19200	Davis Vantage Pro	NA

Save

This section allows configuration of all sub-systems to the Cortexa controller. Any sub-system may be configured to any Com port. The only exception here is HVAC, which must be configured to either Com1 or Com2. The port list will only show the available ports attached to the Cortexa. The Cortexa 7202 comes with four ports, with an expansion board available to add another four, for a total of eight.

EMAIL & WEATHER

SMTP SERVER SETUP

To utilize the Send Mail function within an event, email details must be entered here. Consult your ISP if you do not have the required information.

SMTP Server Setup	
SMTP Host Name	mail.server.com
Recipient Email Address	someone@domain.com
Subject	Home Cortexa

- SMTP Host Name: The address to the SMTP server you are connecting to. This can also be an IP address.
- Recipient Email Address: The E-Mail address that the email will be sent under.
- Subject: The subject line that will be sent with each email.

WEATHER SETUP

The Cortexa can receive weather data from the Internet. The Cortexa will receive weather data for the current day, a five day forecast, and any current local weather watches and warnings.

Weather	
Zip Code	78681 Get Stations
Station Location	Round Rock Fire Dept. 2.05 Miles
Get CVS Data	Note:Select CVS Data above for this to work.
Get Data Every	5 Seconds(s). (Note: 0 = Disable)

Enter your zip code and select the Get Stations button for a list of local weather stations. Then select a station near you for your local weather. Get CVS Data is used with Ambient weather software. This requires Ambient weather software to be configured with a web server.

TIME & LOCATION

Set the current time, date and time zone for the Cortexa. Also, the location of an atomic clock to keep the time synchronized. Note: if the NTP timer server is enabled, you will not be able to manually set the time.

Time / Date	
Time	☐ 11 22 16
Date	☐ 8 11 2003
Time zone	America/Chicago Select the location closest to you
Time update interval	120 Minutes between network time sync.; 300 recommended, or 0 to disable
NTP time server	pool.ntp.org Use a space to separate multiple hosts (only one required)

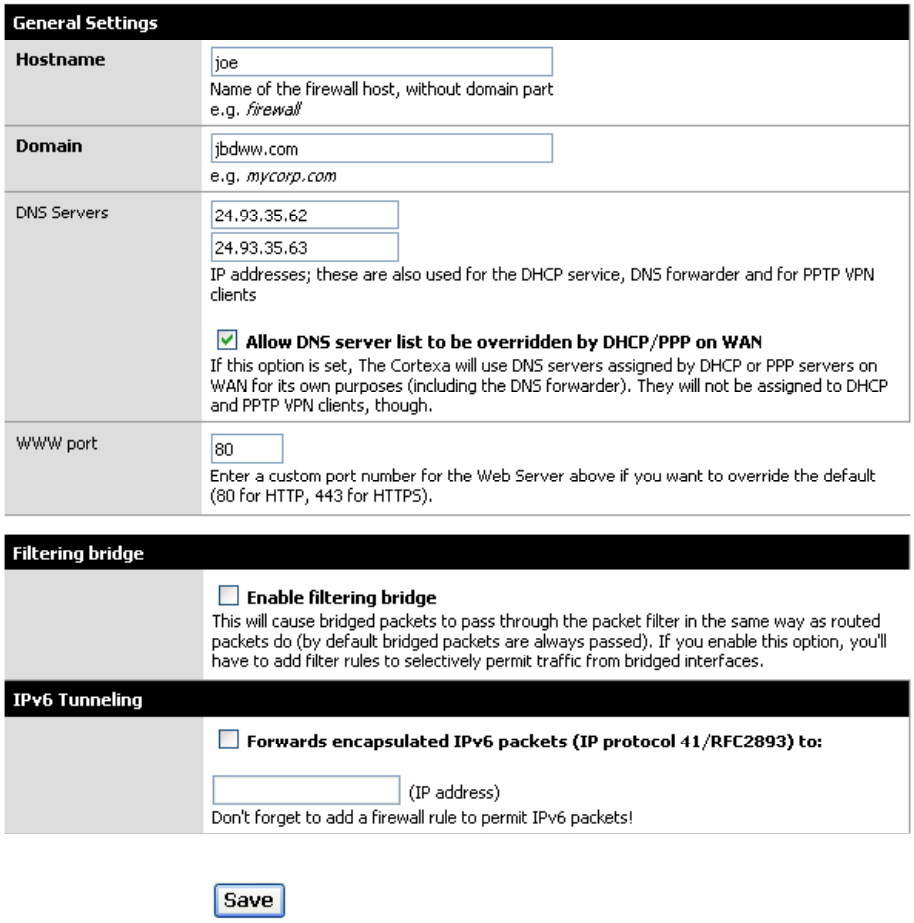
- **Time:** Set the current time
- **Date:** Set the current date
- **Time zone:** Set the current Time Zone you are in
- **Time update interval:** How often the Cortexa will go to the Internet to get the current time
- **NTP Time Server:** The time server from which the Cortexa sources time information

Setting longitude and latitude enables the Cortexa to calculate the current Sunrise and Sunset time. Sunrise and Sunset are often useful triggers for events.

Location	
Longitude	97.444 (Example 97.44)
Latitude	30.165 (Example 30.165)
Sunrise	**07:18:26 AM**
Sunset	**05:32:16 PM**

NETWORK MANAGEMENT

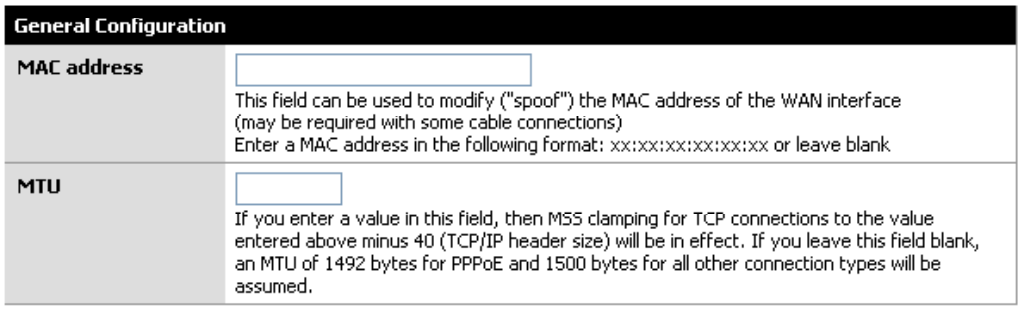
GENERAL SETTINGS



The general settings allow setup of the miscellaneous network information.

- Hostname: The name of the Cortexa 7202. Instead of connecting to the Cortexa 7202 as http://cortexa, you may use http://yourname. Note: The host name must be all one word, no spaces
- Domain: The domain name with which the Cortexa 7202 is associated
- DNS The Domain Name System (DNS) is how the Internet translates domain or website names into Internet address or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to utilize another, enter that IP address in one of these fields.
- WWW Port: The port number to connect to the Cortexa 7202. If using a port other than 80 in the browser to connect, you must specify the port number. For example use: http://cortexa:81 to utilize port 81.

WIDE AREA NETWORK



Media Access Control address: this is a hardware address that uniquely identifies each node of a network

With the MAC address field, you can assign the Cortexa 7202 a MAC address, which is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require that you register the MAC address of your network adapter that is connected to your cable or DSL modem.

Therefore, in order to connect the Cortexa 7202 to your cable or DSL modem instead of the PC (network card or adapter), you must change the Cortexa 7202 MAC to duplicate (or clone) your network card/adapter. You can find your adapter's MAC address by doing the following:

- If you are running Windows 95,98 or Millennium: Go to the **Start, Run,** type in **command**, and press **Enter**. At the DOS prompt type **winipcfg**
- If you are running Windows NT 4.0, 2000 or XP: Go to **Start, Run,** type in **command**, and press **Enter**. At the DOS prompt type **ipconfig /all**.

The Physical Address with 12 digits is your adapter's MAC address. Enter those 12 digits into the MAC Address fields, and click **Apply**. This "clones" your network adapter's MAC address to the Cortexa 7202, and prevents you from having to call your ISP to change the registered MAC address to the adapter's MAC address.

MTU is a limit, expressed in bytes, on the size of data sent over a network. It is the maximum size of a single unit (e.g., an Ethernet frame) of digital communications.

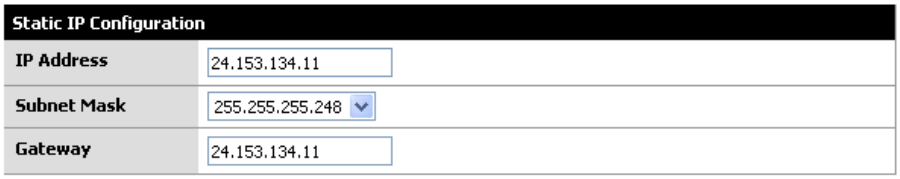
TYPE

The Cortexa 7202 supports three connection types: DHCP (obtain an IP automatically), PPPoE, Static IP Address, and PPPRP. These types are selected from the drop-down menu. The available features will differ depending on what kind of connection type you select. Each option is described below.

STATIC IP

If you are connecting through a static or fixed IP address from your ISP, perform these steps:

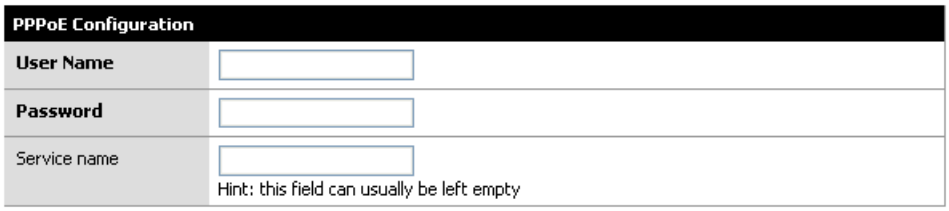
1. Select **Static** IP as the TYPE
2. Enter the IP **Address**
3. Select the **Subnet Mask**
4. Enter the **Gateway**
5. Enter the **DNS** in the 1, and/or 2 fields. You need to enter at least one DNS address
6. Click the **Save** button to save the settings



PPPOE

If you are using DSL and are connecting through PPPoE and if you normally enter a user name and password to access the Internet, perform these steps:

1. Select **PPPoE** as the TYPE
2. Enter the **User Name** provided by your ISP
3. Enter the **Password** provided by your ISP
4. Optionally enter the **Service Name**
5. Click the **Save** button to save the settings



PPTP

PPTP is a service used in Europe only. If you are using a PPTP connection, check with your ISP for the necessary setup information.

PPTP Configuration	
User Name	
Password	
Local IP Address	/ 31
Remote IP Address	

LOCAL AREA NETWORK

LAN Configureation	
IP Address	192.168.4.250
Subnet Mask	255.255.255.0

This is the Cortexa 7202 IP address and Subnet Mask as seen on the internal LAN. The default is 192.168.10.1 for IP address and 255.255.255.0 for Subnet Mask.

OPT1

This option will only appear on the Interfaces menu if a network card is added to the Cortexa

☑ Enable Optional 1 interface

Description	OPT1 Enter a description (name) for the interface here.

IP Configuration	
Bridge With	none
IP Address	192.168.6.250
Subnet Mask	255.255.255.0

The OPT 1 is used for the video server data

The OPT 1 port is like having two separate internal networks

Bridge with: Select the interface that you would like to bridge with. If an interface is selected, then the IP address and Subnet Mask will be the same as the bridged interface.

If you opt not to bridge with another interface, you will need to setup an IP address and Subnet Mask for the new local area network.

You may also change the description of the interface to make it easier to identify when setting up rules and forwards.

NETWORK STATUS

The Status page displays the Cortexa 7202 current status. It reflects the data and selections entered using the setup pages.

WAN Interface	
Status	up
MAC Address	00:40:f4:67:a6:ab
IP Address	24.153.134.38
Subnet Mask	255.255.255.248
Gateway	24.153.134.33
Media	10baseT/UTP
In/Out Packets	133987/127731 (47.79 MB/18.66 MB)

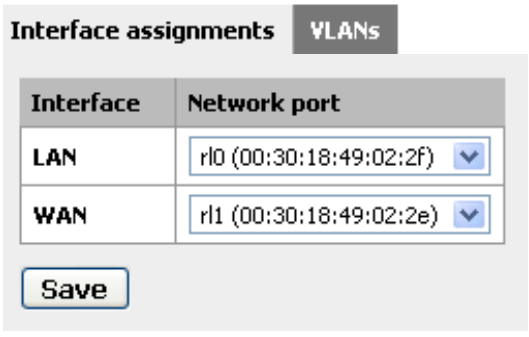
NETWORK TRAFFIC

This allows you to view real-time network traffic on all interfaces, WAN and LAN. In order to utilize this function, install the plug-in as directed. If using Mozilla Firefox, the following step also needs to be performed.

Copy NPSVG6.dll and NPSVG6.zip to your browser's plug-ins folder. These files are normally located in C:\Program Files\Common Files\Adobe\SVG Viewer 6.0\Plugins\

INTERFACE ASSIGNMENTS

This allows you to assign network ports to an Interface. You may also assign Virtual networks.



PING HOST

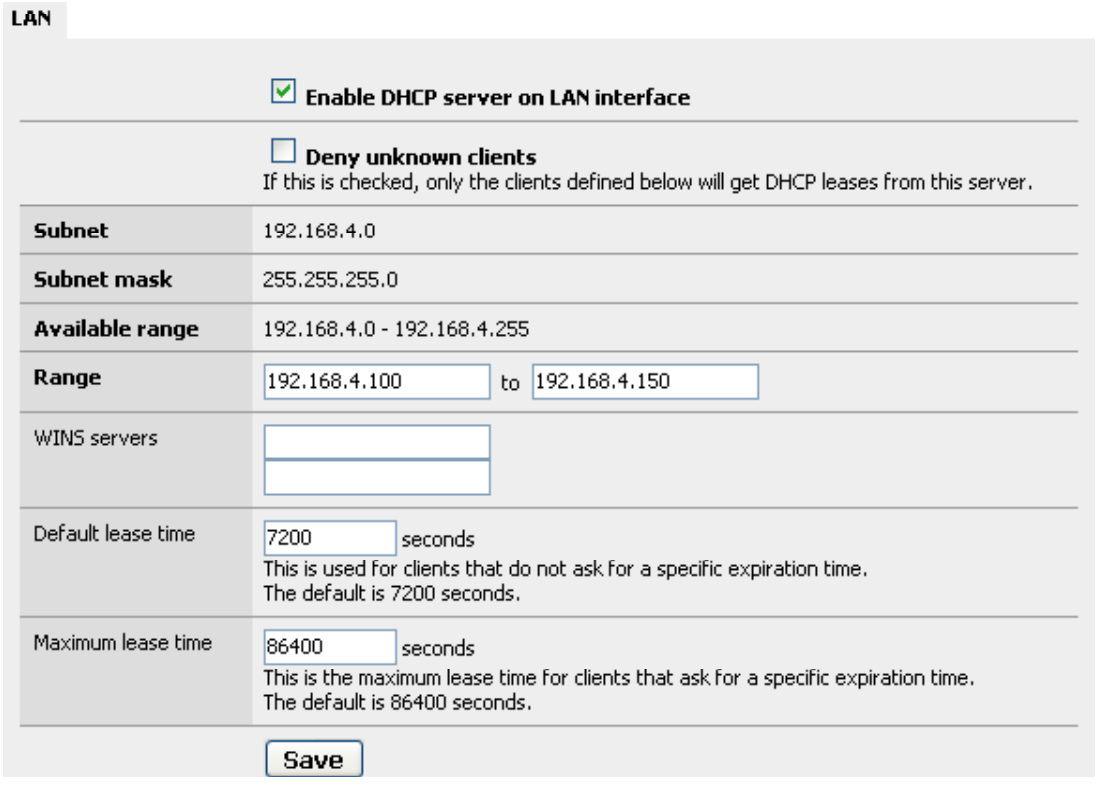
Ping is a trouble-shooting tool to see if you can ping other systems connected to the Cortexa.

SERVICES

DHCP SERVER

The Cortexa can be configured as a DHCP Server from the DHCP Screen. The Dynamic Host Configuration Protocol (DHCP) – A protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network using the Internet's set of protocol (TCP/IP). Each machine that connects to the Internet needs a unique IP address.

When an organization sets up its computer users with a connection, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.



Enabling the DHCP Server

To enable the DHCP server on a particular interface, click on the appropriate tab for the interface and check the "Enable DHCP server on interface" box.

Deny Unknown Clients

With this option selected, the DHCP server will issue IP addresses to known MAC addresses.

Range

In the first box, enter the starting address of your DHCP range. In the second box, enter the ending address of the range. Note that you do not want to make this the same as the available range, as this includes the subnet address and broadcast address, which are unusable. Also, the address of the Cortexa interface cannot be in the range.

WINS Servers

If you use an NT 4 domain, or have pre-Windows 2000 clients that need to access an Active Directory domain, you will need to fill in your WINS server IP addresses in these boxes. If you only have one WINS server, leave the second box blank.

Default and Maximum Lease Time

The default lease time is the length of the DHCP lease on any clients that do not request a specific expiration time on their DHCP lease. The default is 7200 seconds, or two hours. For the vast majority of network environments, this is too low. We recommend setting this to one week; 604,800 seconds.

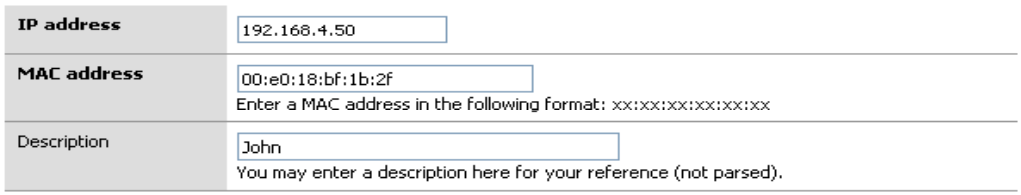
The maximum lease time must be more than the default lease time. Most networks will not use this value at all. In most instances, you can set this to one second longer than the default lease time.

Click **Save** to save your changes, then **Apply** to enable the DHCP server.

STATIC DHCP MAPPING

Static DHCP mappings can be used to assign the same IP address every time to a particular host. This can be helpful if you define access rules on the firewall or on other hosts on your LAN based on IP address, but still want to use DHCP. Alternatively, you can keep the IP address box blank to assign an IP out of the available range, when you are using the "Deny unknown clients" option.

Click the + icon at the bottom of the DHCP configuration page to add a static DHCP mapping.



In the MAC address box, fill in the system's MAC address in the format xx:xx:xx:xx:xx:xx. For Windows NT/2000/XP clients, you can get determine the MAC address by opening up a command prompt and typing 'ipconfig'. For Windows 95/98/ME clients, go to Start, Run, winipcfg. For Unix clients, use ifconfig. In the IP address box, fill in the IP address you want to be assigned to the client, or leave it blank to automatically assign one from the available DHCP range. If you enter a static IP address, it must not be within the range of the DHCP server.

It is recommended you fill in a description in the Description box to remind you what this entry is for, though this is optional.

Click **Save** when you are finished and the mapping will be added.

DNS OVERRIDE

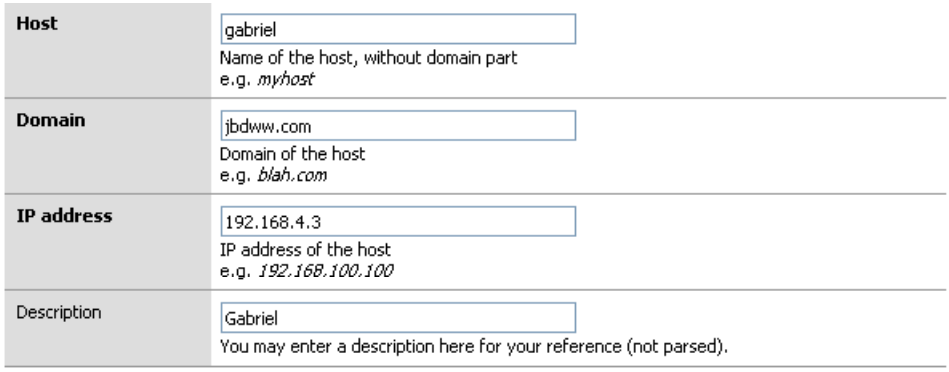
DNS – The Domain Name System (DNS) is the method by which Internet domain names are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember name for an Internet Address.

If there are certain DNS host names you want to override for your internal DNS clients, add them under DNS overrides on this page. For example, if you want www.yourcompany.com to point to a different site internally than it does from the Internet, enter an override for www. yourcompany.com with the appropriate IP address.

This can also be used as a rudimentary, and easy to bypass, filter on web sites LAN clients can visit by assigning the undesired host name to an invalid IP address. For example, to block www.example.com, put in an override to redirect it to an invalid IP address, such as 1.2.3.4. Note that using a different DNS server or editing the hosts file on the client machine gets around this restriction, but doing this is sufficient to block the site for the vast majority of users.

If your Cortexa acts as the DHCP server for your LAN, and you need name resolution between hosts on the LAN, check the “Register DHCP leases in DNS forwarder” box. This will append the default domain in Interfaces: General Setup. For example, if your PC name is my-pc and your default domain is example.com, it will register my-pc.example.com with the IP address assigned from DHCP, so the other hosts on your LAN can locate your machine by that name.

ADDING DNS OVERRIDES

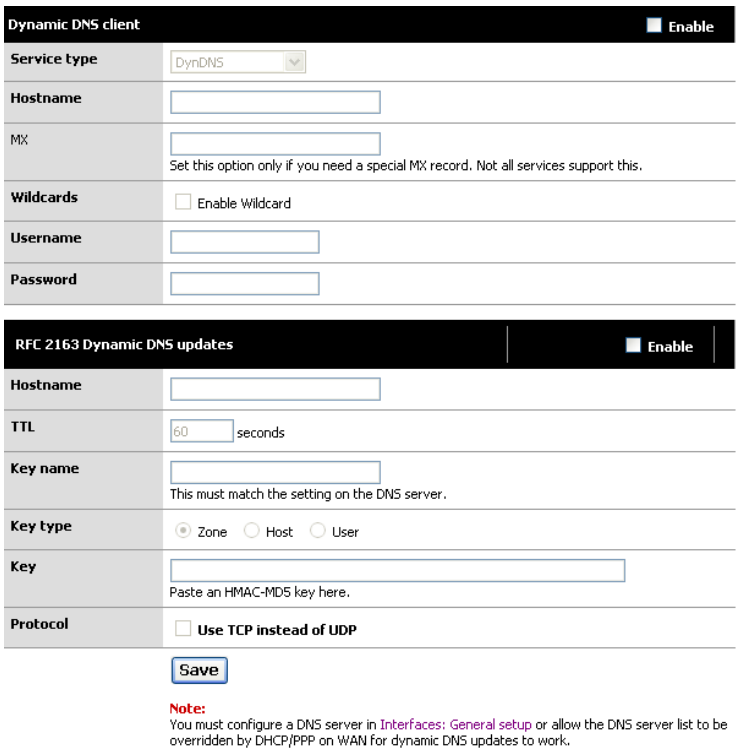


The Edit Screen allows the ability to add and change your current rules.

- **Host**: The host name on the domain without the domain part.
- **Domain**: The domain name of the host.
- **IP**: The new assigned IP address.
- **Description**: Gives the override a name for easy identification.

DYNAMIC DNS

This screen allows you to configure Dynamic DNS. Dynamic DNS gives you the ability to find your Network over the Internet even though you do not have a static IP.



CONFIGURING THE DYNAMIC DNS CLIENT

To start, first check the "Enable Dynamic DNS client" box at the top of the page.

In the "Service type" drop down box, select the service you are using.

Some services support MX DNS records on dynamic DNS sub-domains. This helps ensure you can get email to your host name. If your service supports this (dyndns.org is one that does, others do as well), fill in your mail server's host name in that field. If you do not need an MX record, or if your provider does not support them, just leave the field blank.

Wildcards - If you want to enable wildcard on your dynamic DNS host name, check this box. This means all host names not specifically configured are redirected to your dynamic DNS name. So if your dynamic DNS is example.homeip.net, and you enable wildcards, www.example.homeip.net, mail.example.homeip.net, anything.example.homeip.net, etc. (i.e. *.example.homeip.net) will all resolve to example.homeip.net.

The next two boxes are for your username and password. Enter your account information from the Dynamic DNS provider.

Click **Save**. Your dynamic DNS host name should immediately be updated with your WAN IP address. To verify this, ping your dynamic DNS host name. It should resolve to the IP address of the WAN interface of your Cortexa. If not, check Diagnostics: System Logs for information on why it failed.

PROXY ARP

Proxy ARP means that a particular system, such as a firewall, will respond to ARP requests for hosts other than itself. This can be used to make a firewall mostly disappear from the systems on a network.

For example, if you had a /28 subnet from your ISP that is routed through the Cortexa router, your router appears at the IP of x.x.x.97 with a network address of x.x.x.96 and a broadcast address of x.x.x.111. This leaves a usable chunk of 14 addresses for your hosts.

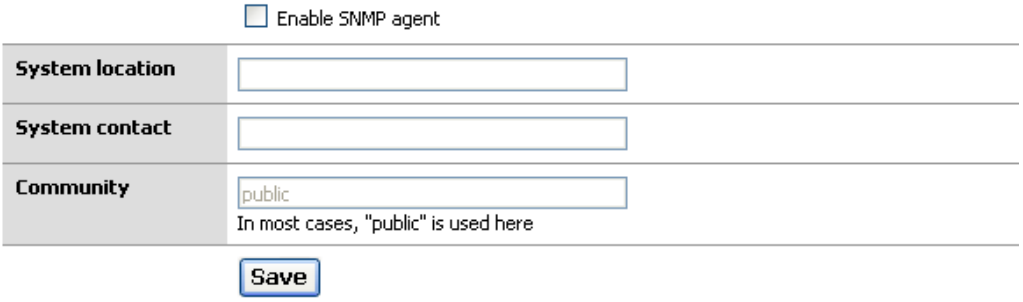
If you wanted to firewall these hosts from the Internet without using Proxy ARP, you would need to subnet your addresses and therefore lose two more addresses for the new network and broadcast, plus half of your remaining IP's would be in the non-firewalled half.

Another method would be to have the firewall do port forwarding between all of the addresses to non-routed IP's (192.168.x.x) for your servers. Done properly, this would be work. It isn't as transparent and may break some protocols like active FTP.

By using Proxy ARP, you can set up your systems in a DMZ to separate them from your client systems. This is also the least invasive method to set up, since you can keep the same IP's on all of the servers as you had when things were not firewalled.

SNMP

You can enable SNMP on your LAN interface on this screen. This is useful if you have a network management or monitoring system that takes advantage of it.



The System location and System contact boxes can be left blank, but can assist you in determining which device you are monitoring if you have several monitored hosts.

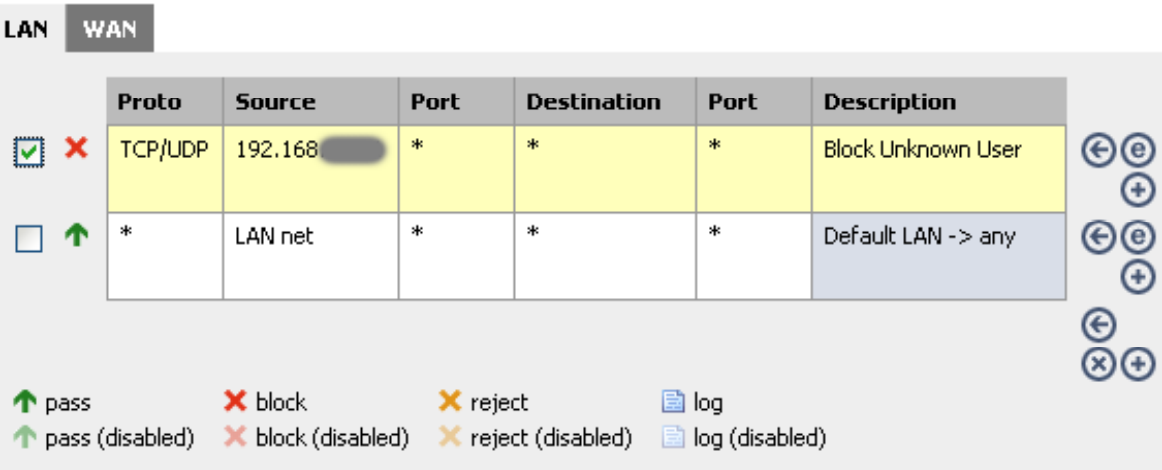
The Community is generally set to public, but if you are concerned about security, you should set this to something difficult to guess, containing numbers and letters. This community name is still passed over the network in clear text, so it could be intercepted, though the most anyone could get with that community name is information on the setup and utilization of your firewall. In most environments, this is likely to be of little to no concern, but is something to keep in mind.

After setting the values as you desire, click Save and your changes will be applied.

FIREWALL

RULES

Rules allow the ability to control the data processed through the Cortexa 7202. This control gives you the option to limit Internet access for specific systems on your network.

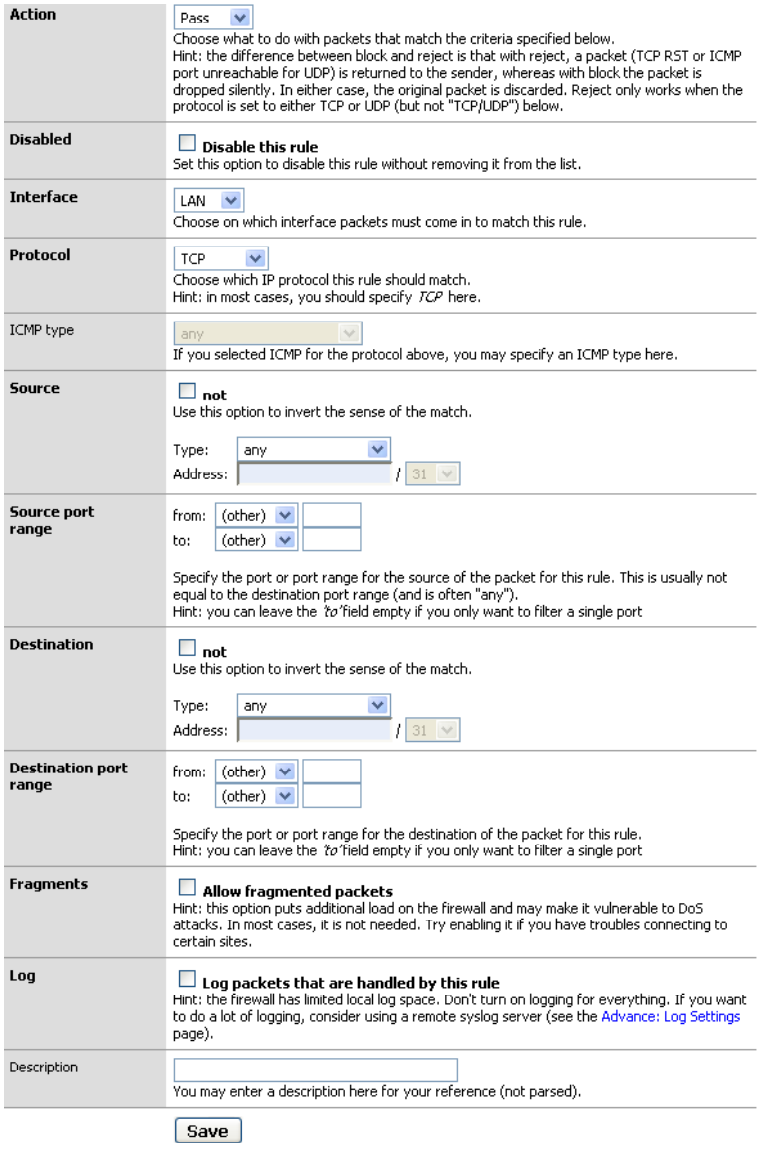


The table shows the following.

- **Proto**: The protocol that is being analyzed
- **Source**: The source of the traffic that is to be analyzed
- **Port**: The port that is being analyzed
- **Destination**: The destinations that the source is allowed to go to
- **Port**: The ports that the source is allowed to connect to
- **Description**: An easy way to identify the rule

Rules may be prioritized with the arrows, and are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay careful attention to the rule order. Everything that is not explicitly passed is blocked by default.

Continued

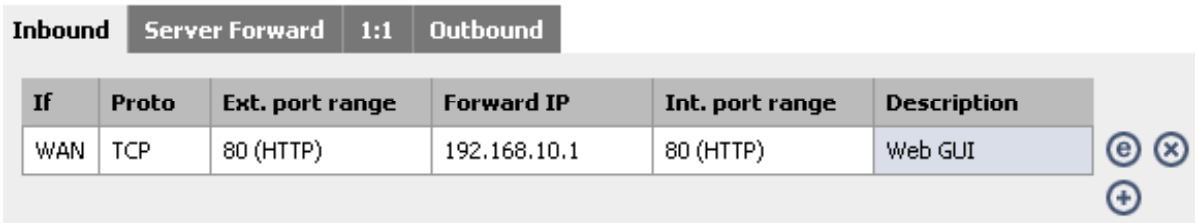


The Edit screen allows the ability to add and change your current rules:

- **Action**: Determines if the rule is a Passing or a Blocking rule.
- **Disable**: Allows you to disable the rule so you can save the settings for a later time.
- **Interface**: The interface that the packets must come in to match this rule.
- **Protocol**: The IP protocol that the packets must match for this rule.
- **Source**: Packet source.
- **Source Port Range**: The port that the packet is on and must match for this rule.
- **Destination**: Destination address the packets are trying to reach and if matched, will be denied.
- **Destination Port Range**: The range of ports that are allowed for this rule.
- **Fragments**: Allows fractional packets to pass through.
- **Description**: Gives the rule a name to help find it.

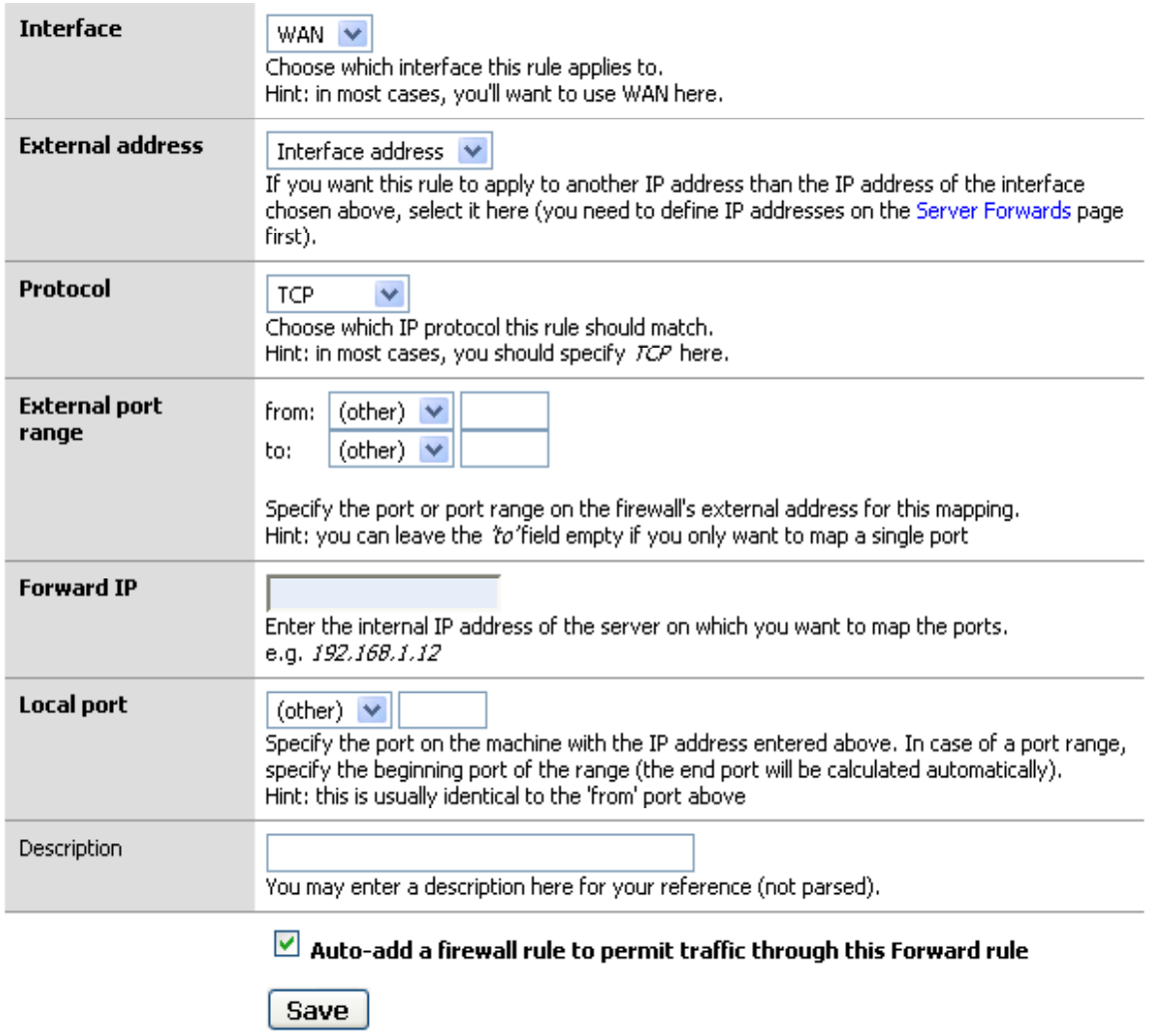
FORWARDS

INBOUND FORWARDS



Forwards Rules allow you to set up public services on your network, such as web servers, ftp servers, or e-mail servers. When users send this type of request to the network via the Internet, the Cortexa 7202 will forward those requests to the appropriate PC.

ADDING INBOUND FORWARDS



Interface

Interface is generally set to WAN in order to permit traffic coming from the Internet. You can also select any optional interfaces here.

Optional interfaces might be useful on a DMZ interface to allow access from the DMZ to a port on a host on your LAN. For example, if you want to use a LAN DNS server, you could put an Inbound NAT rule in on the DMZ interface opening UDP port 72 to your DNS server's LAN IP address, and use Cortexa's DMZ interface IP address as your DNS server on DMZ hosts. There is no real advantage doing this versus putting in a firewall rule to permit this traffic, and using the LAN IP address of the DNS server.

External address

External address is set to the WAN interface IP address. If you have multiple public IP's, you can use other addresses here that you have previously defined on the Server NAT tab.

Protocol

Choose which IP protocol the service you are using requires, TCP, UDP or TCP and UDP.

External port range

Either select the desired protocol from the drop down box, or type in the port range in the text boxes. You can leave the "to" field empty if you only want to map a single port.

Forward IP

This is the internal IP address of the machine to which you are mapping the ports. In the given example, the LAN IP address of the web server is 192.168.10.4. This can also be a host on an optional network, and ideally it will be to a host on a DMZ. You should avoid opening ports to your LAN if possible.

Local port

This is the port on the Forward IP defined above to which we want to translate the connection. In this case it is the same as the external port, but it doesn't have to be.

Description

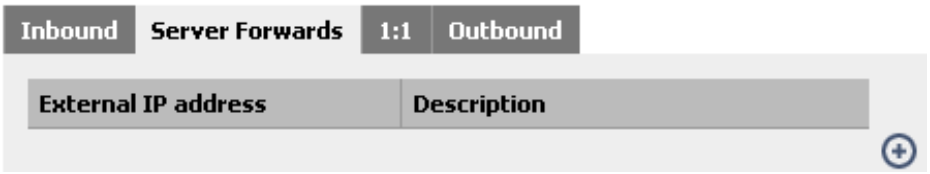
Optional, however we strongly recommend putting in a description so you remember the purpose of this entry, and to make your rules easier to read and comprehend.

Auto-add a firewall rule to permit traffic through this Forward rule

We recommend you check this box in all circumstances. If you need to tighten the default rule, you can do so later. If you don't let the webGUI create the rule automatically, it's more likely to be incorrect or problematic.

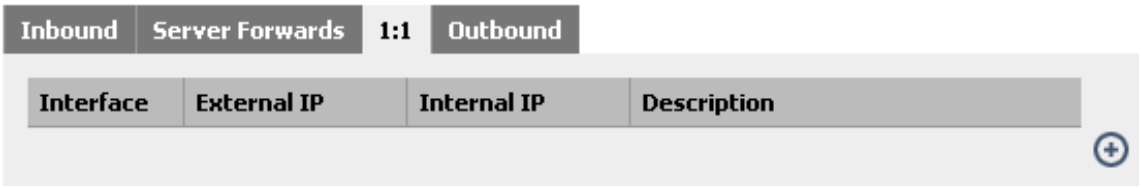
Click **Save**, then **Apply Changes**. You will then see the result, similar to the following.

SERVER FORWARDS



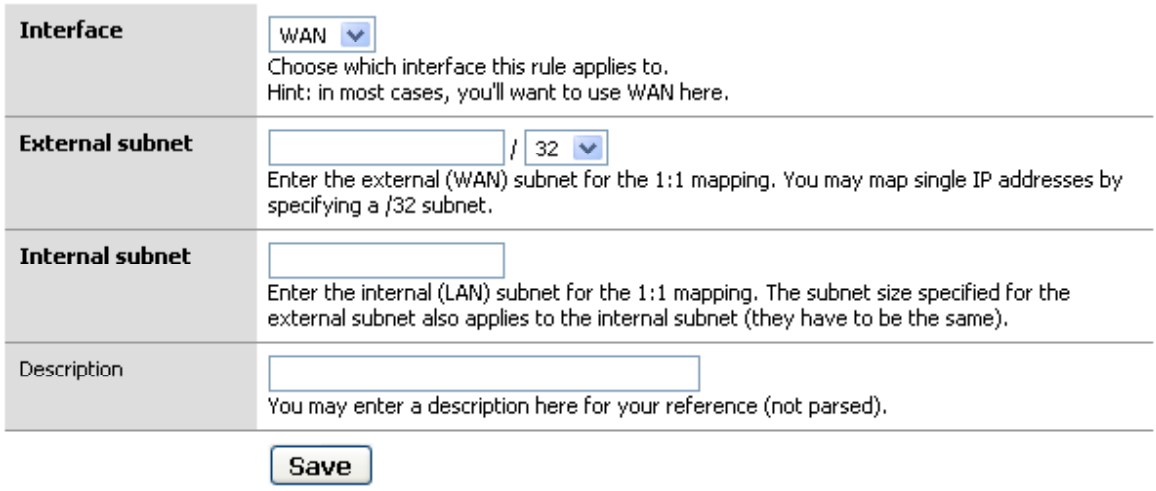
If you want to use a public IP address other than the WAN interface address with Inbound Forwards, you need to define the address in Server Forwards first.

1:1 FORWARD



1:1 Forward maps an internal IP to external IP, generally mapping a public IP address to a private IP address and vice versa. When you assign a 1:1 Forward mapping, any traffic coming from that host to the Internet will be NAT'ed to the defined external IP, and any traffic coming into the external IP will be NAT'ed and passed to the internal IP if firewall rules permit. (by default, the firewall rules do not allow any inbound traffic to 1:1 Forward mappings). You can also map entire subnets with one entry.

ADDING 1:1 FORWARDS



Interface

Interface will be WAN in most cases.

External IP

The external IP will be set to the IP address you wish to map.

Internal subnet

In most cases this will be a single IP address on either your LAN or an optional interface like a DMZ.

Description

Description is optional but recommended. After verifying your entries, click **Save** and **Apply Changes.**

ALIASES

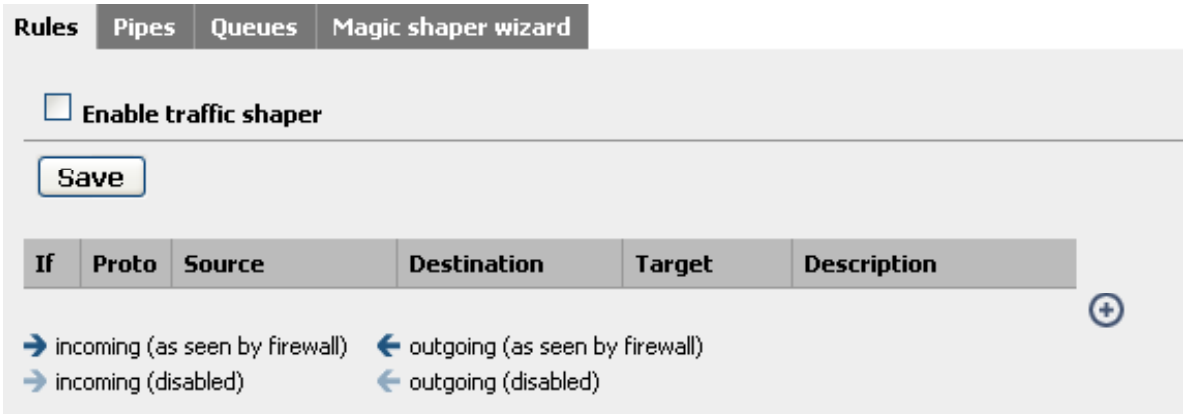
Aliases act as placeholders for real IP addresses and can be used to minimize the number of changes that have to be made if a host or network address changes. You can enter the name of an alias instead of an IP address in all address fields that have a blue background. The alias will be resolved to its current address according to the list below. If an alias cannot be resolved, e.g. because it has been deleted, the corresponding element will be considered invalid and skipped.

STATIC ROUTE

Paths through the network must be found and made available to the router so it knows the best path on which to forward a packet to its destination. Static routing is the process a network administrator uses to manually configure network routes.

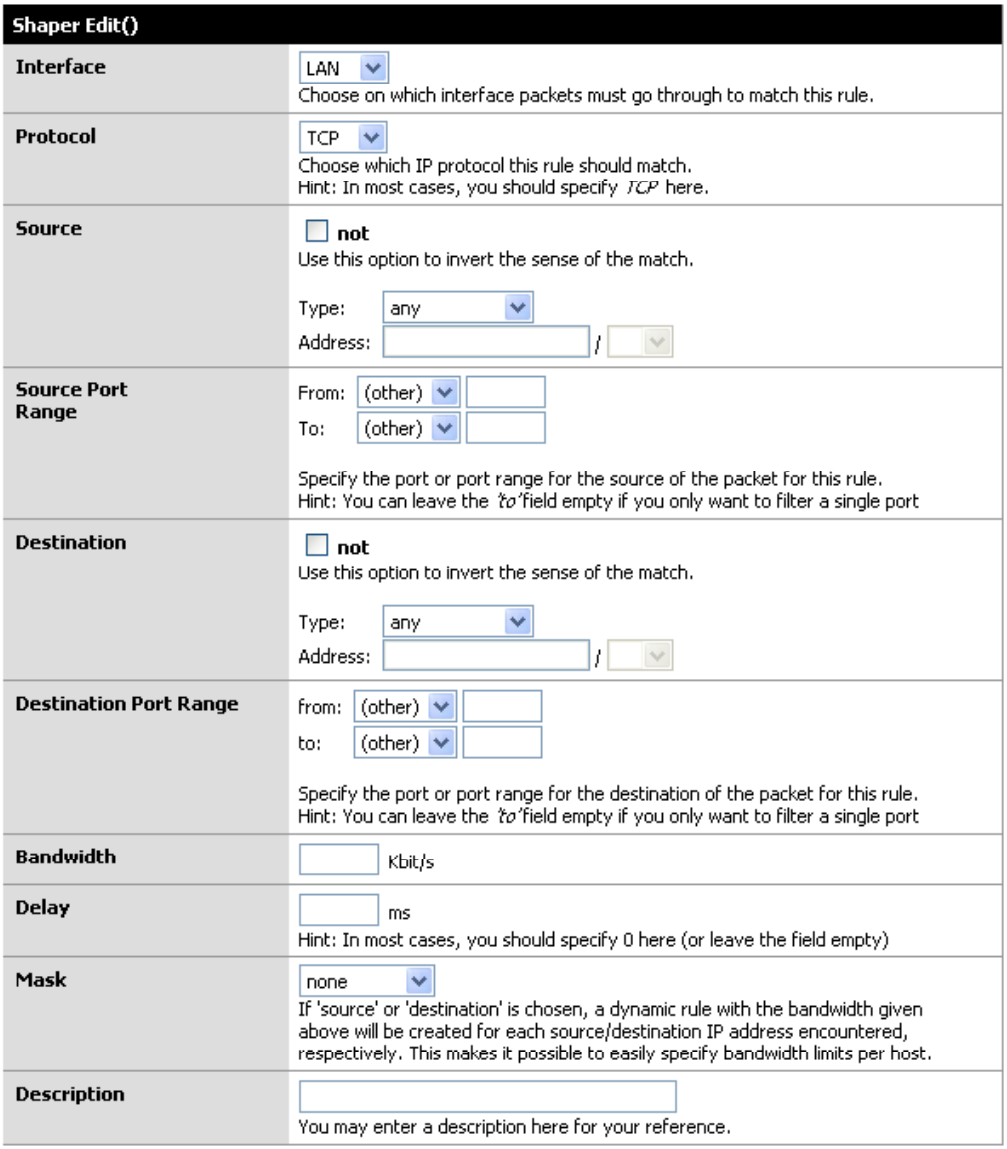
TRAFFIC SHAPER

Traffic shaping gives you the ability to allow a specific amount of bandwidth for each device on the LAN.



Current Rules:

- If: The interface packets must go through
- Proto: The protocol being analyzed
- Source: The source of the traffic to be analyzed
- Port: The port being analyzed
- Destination: The destination being analyzed
- Port: The destination port being analyzed
- Bandwidth: The amount of bandwidth allowed for this rule
- Delay: The amount of delay before packets are allowed through
- Mask: Dynamic rule with the bandwidth given above
- Description: An easy way to identify the rule



The Edit screen allows the ability to add and change current Rules:

- **Interface:** The interface packets must match
- **Protocol:** The IP protocol packets must match
- **Source:** The source of the packets must match. You may use the "not" function so everything else will match, but not the source
- **Source Port Range:** The port the packet is on must match
- **Destination:** The destination address that the packets are trying to reach and, if matched, the packets will be shaped
- **Destination Port Range:** If the ports are matched, the packets will be shaped
- **Bandwidth:** The amount of bandwidth that is allowed
- **Delay:** Holds the packets for a specific amount of time. In most cases it is 0 or blank

- **Mask:** If 'source' or 'destination' is chosen, a dynamic rule with the bandwidth given above will be created for each source/destination IP address encountered respectively, which makes it possible to easily specify bandwidth limits per host
- **Description:** Gives the rule a name to make them easier to locate

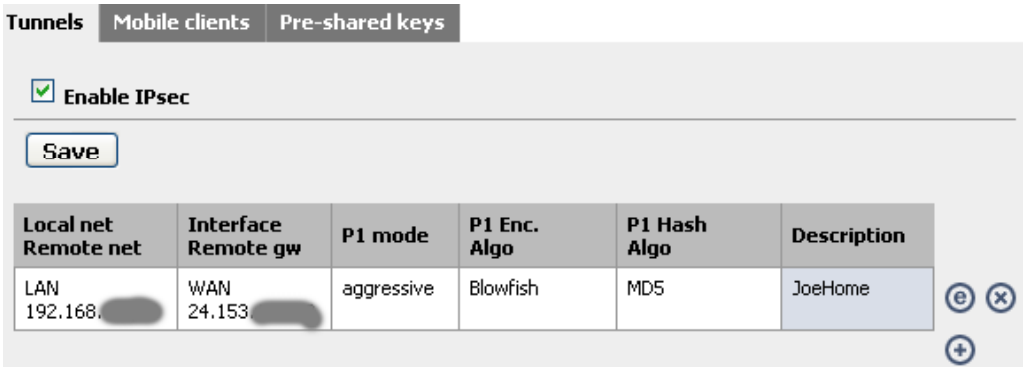
VPN (VIRTUAL PRIVATE NETWORK)

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. The connection is very specific as far as its settings are concerned; and creates the security. The VPN screen allows you to configure your VPN setting to make your network more secure.

IPSEC

This is used if you decide to build an IPSEC tunnel between your firewall and some other network. The most common uses we see are connecting home networks to the office, or setting up private WANs.

There is only one section of the Cortexa interface that you need to use to do this.



Now we need to add a VPN connection, to do this click on the ⊕ icon.

The first area is the one you use to establish what network ranges will use this IPSEC tunnel.

Continued

Mode	Tunnel
Disabled	☐ **Disable this tunnel** Set this option to disable this tunnel without removing it from the list.
Auto-establish	☑ **Automatically establish this tunnel** Set this option to automatically re-establish this tunnel after reboots/reconfigures. If this is not set, the tunnel is established on demand.
Interface	WAN Select the interface for the local endpoint of this tunnel.
Local subnet	Type: LAN subnet Address: / 0
Remote subnet	192.168.10.1 / 24
Remote gateway	70.112.[redacted] Enter the public IP address of the remote gateway
Description	Casa Automation You may enter a description here for your reference (not parsed).

This is the first set of fields that we need to concentrate on. Later, when testing your tunnel, you can actually fail to establish level 2 connection if this data is incorrect. We will note what to pay particular attention to as we go along.

1. **Mode**: This cannot be changed.
2. **Disabled**: This is an "on / off" button if you need to disable the tunnel for whatever reason. Simply select the edit or ⓔ from the main VPN: IPsec window and click this checkbox element, then select Apply at the bottom of the page. When you need the tunnel again, reverse the process.
3. **Interface**: This is how you determine which part of your network will be the termination point end point for the VPN Tunnel. If you are connecting to a remote server, then WAN is your option.
4. **Local subnet**. This is where you can set which parts, hosts, or the entire LAN, can be accessed from the other side of the VPN tunnel. The easiest thing to do is to set the LAN subnet as the option; this means your entire LAN will be accessible from the remote network. IMPORTANT: The other end of the tunnel has this same field. Make sure the other end is set exactly as you set this end. For example, if you selected "Single host" in this section and entered the IP address of that host, the other person would set that host in their "Remote Subnet" field.

5. **Remote Subnet.** This is more than just labeling which host(s) you want to access on the other network. As mentioned in item 4 it is paramount that you set this exactly like the "local subnet" section. If not, level 2 of the VPN connection will fail and traffic will not pass from one VPN segment to the other.
6. **Description**: We strongly encourage some documentation here.

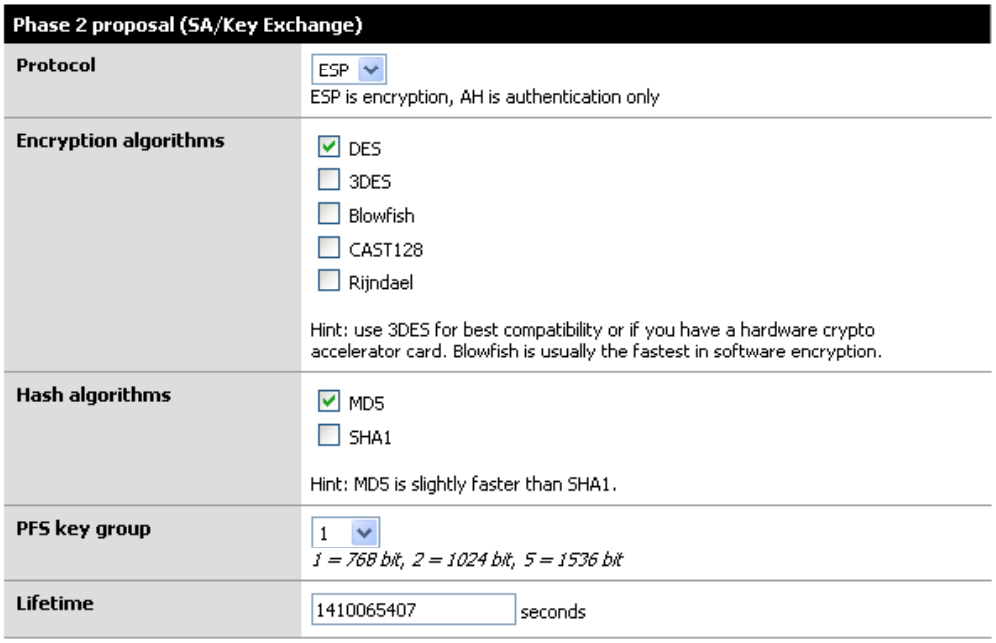
Now that the basics for the routing have been established. We can now move to phase 1 of the VPN authentication process.

Phase 1 proposal (Authentication)	
Negotiation mode	main Aggressive is faster, but less secure.
My identifier	IP address 24.153.134.10
Encryption algorithm	DES Must match the setting chosen on the remote side.
Hash algorithm	MD5 Must match the setting chosen on the remote side.
DH key group	1 *1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit* Must match the setting chosen on the remote side.
Lifetime	1410065407 seconds
Pre-Shared Key	jdoran812

Here, and even in phase 2, it is vital to ensure both VPN servers have EXACTLY the same settings for all of these fields.

1. **Negotiation mode:** This is the type of authentication security that will be used. Unless you are extremely concerned about security, leave this as aggressive. It is significantly faster and will ensure that your VPN tunnel will rebuild itself quickly and probably won't timeout an application if the tunnel was down when the resource on the other end was requested.
2. **My Identifier**: This is the key to probably 90% of problems where the VPN tunnel is not established. Very simply, set your identifier to something that isn't going to change. So if you leave it as My IP address, then make sure that IP is static and persistent. If you use a DHCP assigned address then we suggest using domain name instead. This is because the domain name can be completely your own, even if you do not own the domain name.

3. **Encryption Algorithm**: 3DES is the de facto standard if you are connecting to another Cortexa, or a system that will support it, change this to Blowfish. It is more secure and about twice as fast! If you are trying to connect to a VPN device that only supports DES then you will need to downgrade and hope no one decrypts your key exchange. MAKE SURE BOTH VPN DEVICES ARE USING THE SAME ENCRYPTION ALGORITHM.
4. **Hash Algorithm**: this is the hash used for checksum. MD5 is a good choice, SHA1 is another algorithm, but not everything supports it. Again make sure you are using the same setting as the other end of the tunnel.
5. **DH Key Group**: Most systems will support at least up to 1024 bit. This is what we recommend using.
6. **Lifetime**: This field is more important than it appears. This lifetime, as opposed to the one in phase 2, is how long your end will wait for phase 1 to be completed. We suggest using 28,800 in this field.
7. **Pre-Shared Key**: This key must be exactly the same on both VPN routers. It is case sensitive, and it does support special characters. We suggest using both.

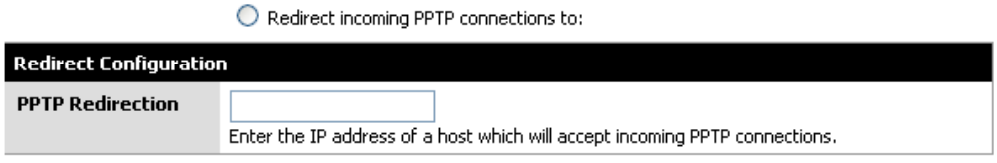


Phase 2 is what builds the actual tunnel, sets the protocol to use, and sets the length of time to keep the tunnel up when there is no traffic on it.

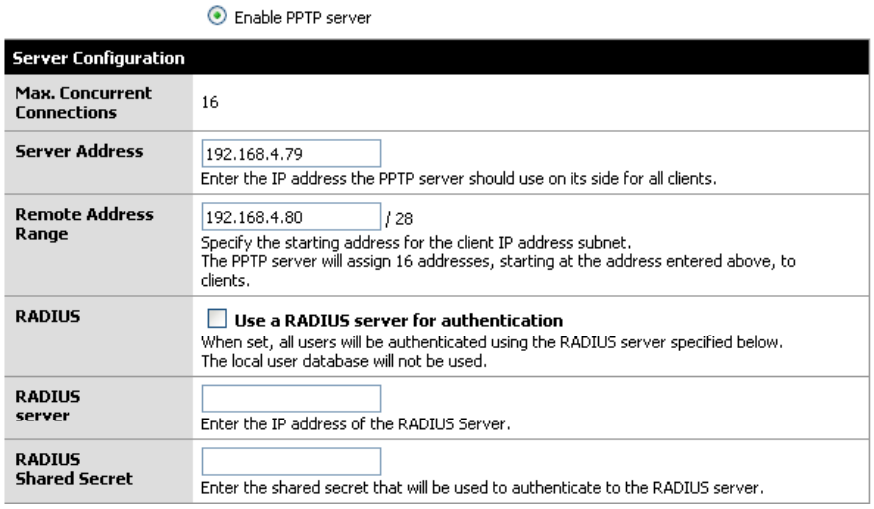
1. **Protocol**: ESP is the de facto VPN transport protocol. We suggest leaving this as is. Note: The system should auto-generate a firewall rule for you to allow ESP or AH to the endpoint of the VPN. We will check this later. If it does not, you will need to make a firewall rule allowing ESP (or AH if you changed this) traffic to the interface you established as your end point of the tunnel. We will outline that later.
2. **Encryption algorithms**: As before in phase 1, make sure you are setting the algorithm exactly as it is set on the other VPN server. You can use several, and when you do so everything you select is available for use. We recommend keeping things simple so only check the one you are going to use.
3. **Hash algorithms**: Just as in phase 1, make sure your selected hash matches on both ends. And as in step 2, don't add things you don't need. SHA1 is the suggestion if you can, but MD5 is always a good alternative.
4. **PFS key group**: this works exactly like it does in phase 1. We suggest using 1024 bit, the default is off.
5. **Lifetime**: This is the lifetime the negotiated keys will be valid for. Do not set this to too high. We suggest one day, 86,400. A value larger than this will be less secure.

PPTP

PPTP *Point to Point Tunneling Protocol* – A protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. PPTP does not specify any changes to the PPP protocol, but rather describes a "tunneling service" for carrying PPP (a tunneling service is any network service enabled by tunneling protocols such as PP2P, L2F, L2TP , and IPSEC tunnel mode). One example of a tunneling service is secure access from a remote small office network to a headquarters corporate intranet via a Virtual Private Network (VPN) that traverses the Internet. However, tunneling services are not restricted to corporate environments and may also be used for personal (i.e., non-business) applications.



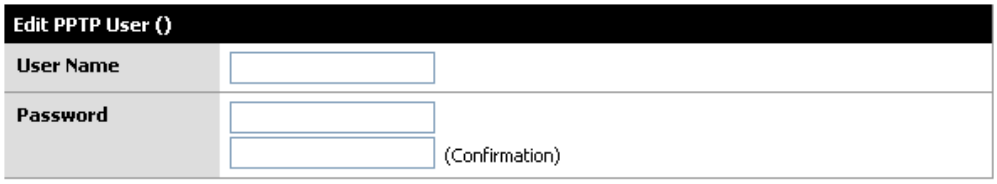
If you have your own internal PPTP server, you may redirect the PPTP request to your internal PPTP server.



- **Max Connections:** The maximum allowed tunnels at any time
- **Server Address:** The IP address that the PPTP server should use for all clients
- **Remote Address Range:** The range of IP addresses given to clients
- **RADIUS:** If you wish to use a RADUIS server to handle all users' authentications
- **RADIUS server:** The IP address of the RADIUS Server
- **RADIUS Shared Secret:** The shared secret that the RADIUS server is using

PPTP USERS

Allows you to add PPTP users to gain access to the network through the PPTP tunnel.



GETTING STARTED

To use Cortexa Audio Player you will need to:

1. Make sure you have iTunes installed on a PC.
2. Make sure your Cortexa LAN is configured correctly.
3. Make sure the PC or MAC running iTunes is communicating directly to the Cortexa on the LAN.
4. Enable Music Sharing features in iTunes Preferences menu.

Read on for detailed explanations of the above steps.

WHAT IS THE "CORTEXA AUDIO PLAYER?"

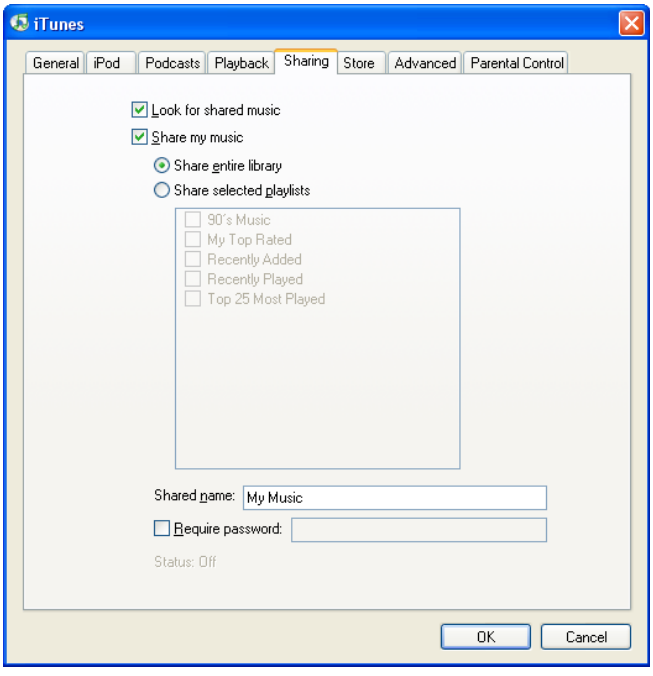
The Cortexa Audio Player is a networked audio player. It does not, in itself, store any music files. It plays files stored on a computer connected to your local area network. To play the music files, the Cortexa interfaces with iTunes software installed on your computer. The Audio Player is controlled by a friendly user interface allowing the selection of playlists, artists, album and genres.

INSTRUCTIONS FOR INSTALLING ITUNES

1. If you do not already have iTunes, download and install it from www.itunes.com. Cortexa Audio Player requires v. 4.0 or later.
2. Enable Music Sharing in iTunes.

ENABLING MUSIC SHARING IN ITUNES

To turn on the Music Sharing option, select iTunes/Preferences menu (Mac) or Edit/Preferences (PC). In the dialog box that appears, click the Sharing tab. Check the "Share My Music" option to enable sharing across your local network. Do not close iTunes, or you will lose the connection to the Cortexa. iTunes must be running at all times to use the Cortexa Audio Player. Leave the Require password option blank.



Continued

PERSONAL FIREWALL SETUP

If you have trouble connecting and your computer has a firewall installed, make sure your firewall is configured to allow iTunes music sharing:

Mac: Open System Preferences. Select the Sharing icon and click on the Firewall tab. Select the option "iTunes Music Sharing."

PC: Refer to your firewall's documentation for opening incoming ports. Configure your firewall to allow incoming connections on port 3689. For WindowsXP service Pack 2 users, open "Security Center," and click on "Windows Firewall" on the bottom right of the window. In the window that pops up, click on the Exceptions tab, and check to see weather iTunes is shown and checked in the list of Programs and Services. If not, press "Add Program" and add iTunes.

NETWORK TROUBLESHOOTING

This appendix consists of frequently asked questions, and may provide possible solutions to problems regarding the installation and operation of the Cortexa.

If you need further support, please contact us at support@cortexatechnology.com.

I need to set a static IP address on a PC

The Cortexa, by default, assigns an IP address range of 192.168.10.100 to 192.168.10.150 using the DHCP server in the Cortexa. To set a static IP address, you can only use the ranges 192.168.10.2 to 192.168.10.99 and 192.168.10.151 to 192.168.10.254. Each PC or network device that uses TCP/IP must have a unique address to identify itself in a network. If the IP address is not unique to a network, Windows will generate an IP conflict error message. You can assign a static IP address to a PC by performing the following steps:

For Windows 95, 98, and Me:

A. Click **Start, Settings,** and **Control Panel**. Double-click **Network**.
B. In *The following network components are installed* box, select the **TCP/IP->**associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the **Properties** button.
C. In the *TCP/IP properties* window, select the **IP address** tab, and select **Specify an IP address**. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.10.2 to 192.168.10.99 and 192.168.10.151 to 192.168.10.254. Make sure that each IP address is unique for each PC or network device.
D. Click the **Gateway** tab, and in the *New Gateway* prompt, enter **192.168.10.1**, which is the Cortexa's default IP address. Click the **Add** button to accept the entry.
E. Click the **DNS** tab, and make sure the **DNS Enabled** option is selected. Enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Enter the **DNS entry 192.168.10.1** (Cortexa's default IP address).
F. Click the **OK** button in the *TCP/IP properties* window, and click **Close** or the **OK** button for the Network window.
G. Restart the computer when asked.

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

A. Click **Start, Settings,** and **Control Panel**. Double-click **Network and Dial-Up Connections**.
B. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
C. In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP),** and click the **Properties** button. Select **Use the following IP address** option.
D. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.10.2 to 192.168.10.99 and 192.168.10.151 to 192.168.10.254.
E. Enter the Subnet Mask, **255.255.255.0**.
F. Enter the Default Gateway, **192.168.10.1** (Cortexa's default IP address).
G. Toward the bottom of the window, select **Use the following DNS server addresses,** and enter the **Preferred DNS server,** 192.168.10.1 (Cortexa's default IP address).
H. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
I. Restart the computer if asked.

For Windows NT 4.0:

A. Click **Start, Settings,** and **Control Panel**. Double-click the **Network** icon.
B. Click the **Protocol** tab, and double-click **TCP/IP Protocol**.
C. When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter.
D. Select **Specify an IP address,** and enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
E. Enter the Subnet Mask, **255.255.255.0**.

Continued

F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).

G. Click the **DNS** tab, and enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Under DNS Service Search Order, click the **Add** button. Enter the **DNS IP address 192.168.10.1** (Cortexa's default IP address) in the DNS Server field, and click the **Add** button.

H. Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.

I. Restart the computer if asked.

I want to test my Internet connection

A. Check your TCP/IP settings.

For Windows 95, 98, and Me:

Make sure **Obtain IP address automatically** is selected in the settings.

For Windows 2000:

- Click **Start, Settings,** and **Control Panel**. Double-click **Network and Dial-Up Connections**.
- Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
- In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP),** and click the **Properties** button. Make sure 58 that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
- Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the Local Area Connection Properties window.

- Restart the computer if asked.

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

- Click **Start** and **Control Panel**.
- Click the **Network and Internet Connections** icon and then the **Network Connections** icon. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
- In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
- Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
- Restart the computer if asked.

For Windows NT 4.0:

- Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
- Click the **Protocol** tab, and double-click on **TCP/IP Protocol**.
- When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter and set it for **Obtain an IP address from a DHCP server**.
- Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.
- Restart the computer if asked.

B. Open a command prompt.

- For **Windows 95, 98,** and Windows **Me,** click **Start** and **Run**. In the Open field, type in **command**. Press the **Enter** key or click the **OK** button.

- For **Windows NT, 2000,** and **XP,** please click **Start** and **Run**. In the Open field,

type **cmd**. Press the **Enter** key or click the **OK** button.

C. In the command prompt, type **ping 192.168.10.1** and press the **Enter** key.

- If you get a reply, the computer is communicating with the Cortexa.
- If you do NOT get a reply, please check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.

D. In the command prompt, type **ping** *followed by your WAN IP address* and press the **Enter** key. The WAN IP Address can be found in Cortexa's Web-based Utility. For example, if your WAN IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.

- If you get a reply, the computer is connected to the Cortexa.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

E. In the command prompt, type **ping www.yahoo.com** and press the **Enter** key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a web page, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

I am not getting an IP address on the WAN with my Internet connection

A. Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
B. If you need to register the MAC address of your Ethernet adapter with your ISP, please see "Appendix G: Finding the MAC address and IP Address for Your Ethernet Adapter." If you need to clone the MAC address of your Ethernet adapter onto the Cortexa, see the MAC Address Clone section of "Section 6.2.2: WAN" for

details.

C. Make sure you are using the right WAN settings. Contact your ISP to see if your WAN connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of "Section 6.2.2: WAN" for details on WAN settings.
D. Make sure you have the right cable. Check to see if the WAN port has a solidly lit Link LED.
E. Make sure the cable connecting from your cable or DSL modem is connected to the Cortexa's LAN 1 port. Verify that the Status page of the Cortexa's Web-based Utility shows a valid IP address from your ISP.
F. Turn off the computer, Cortexa, and cable/DSL modem. Wait 30 seconds, and then turn on the Cortexa, cable/DSL modem, and computer. Check the Status tab of the Cortexa's Web-based Utility to see if you get an IP address.

I am not able to access the Web-based Utility's Setup page

A. Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Cortexa.
B. Refer to "Appendix G: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
C. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."
D. Refer to "Problem #6: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

I need to set up a server behind my Router

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed. Follow these steps to set up port forwarding through the Cortexa's Web-based Utility. We will be setting up web, ftp, and mail servers.

A. Open the Router's Web-based Utility, as shown in "Section 6:" and go to the **Advanced section.**
B. Now select **forwards** under the Firewall column.
C. With the Inbound tab selected, click on the ⊕ button.
D. Select the **Protocol** type for the packets.
E. Either select an existing port, or place your own custom port in.
F. Put the IP address of the server in the Forwards IP box.
G. Select the port to forward the packets to. Most of the time this should be the same as the External Port.
H. Give the forwarding rule a **description** to make it easy to find.
I. Select **auto-add** to make the rule work right away.
J. When you have completed the configuration, click the **Save** button.

I am a PPPoE user, and I need to remove the proxy settings or the dial-up popup window

If you have proxy settings, you need to disable these on your computer. Because the Cortexa is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:

A. Click **Start, Settings,** and **Control Panel.** Double-click **Internet Options.**
B. Click the **Connections** tab.
C. Click the **LAN settings** button and remove anything that is checked.
D. Click the **OK** button to go back to the previous screen.
E. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:

A. Start **Netscape Navigator,** and click **Edit, Preferences, Advanced,** and **Proxies.**
B. Make sure you have **Direct connection to the Internet** selected on this screen.

C. Close all the windows to finish.

I can't access my email, web, or VPN, or I am getting corrupted data from the Internet

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. Most DSL users should use MTU 1492. If you are having some difficulties, perform the following steps:

A. To connect to the Cortexa, go to the Web-based Utility, as shown in "Section 6.2".
B. Click the **Advanced => Wan** tab.
C. Look for the MTU option, and in the Size field, enter **1492**.
D. Click the **Save** button to continue.

If your difficulties continue, change the **Size** to different values. Try this list of values, one value at a time, in this order, until your problem is solved:

1462
1400
1362
1300

When I enter a URL or IP address, I get a time-out error or am prompted to retry

A. Check if other PCs work. If they do, ensure that your workstation's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
B. If the PCs are configured correctly, but still not working, check the Cortexa. Verify that it is connected and ON. (If you cannot connect to it, check the LAN and power connections.)
C. If the Cortexa is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Cortexa to verify a direct connection.
D. Manually configure the TCP/IP with a DNS address provided by your ISP.
E. Make sure that your browser is set to connect directly and that any dial-

up is disabled. For Internet Explorer, click **Tools, Internet Options,** and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit, Preferences, Advanced,** and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

What is the maximum number of IP addresses that the Router will support?

Cortexa will support up to 272 IP addresses.

Where is the Cortexa installed on the network?

In a typical environment, the Cortexa is installed between the cable/DSL modem and the LAN. Plug the Cortexa into the cable/DSL modem's Ethernet port.

Does the Cortexa support IPX or AppleTalk?

No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from WAN to LAN.

Does the Cortexa's WAN connection support 100 Mbps Ethernet?

Yes, it does support 100 Mbps over its auto-sensing 10/100 port.

What is Network Address Translation and what is it used for?

Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since

the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with Internet accounts such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

I am not able to access Cortexa's Web-based Utility. What can I do?

You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

Does the Cortexa pass PPTP packets or actively route PPTP sessions?

The Cortexa allows PPTP packets to pass through.

Does the Cortexa replace a modem? Is there a cable or DSL modem in the Cortexa?

No, the Cortexa must work in conjunction with a cable or DSL modem.

INSTALLING THE TCP/IP PROTOCOL

Follow these instructions to install the TCP/IP Protocol on one of your PCs *only* after a network card has been successfully installed inside the PC. These instructions are for Windows 95, 98, and Millennium. For TCP/IP setup under Windows NT, 2000, or XP, please refer to your Windows documentation.

1. Click the **Start** button. Choose **Settings,** and then **Control Panel**.
2. Double-click the **Network** icon. Your Network window should pop up. Select the **Configuration** tab.

3. Click the **Add** button.
4. Double-click **Protocol**.
5. Highlight **Microsoft** under the list of manufacturers.
6. Find and double-click **TCP/IP** in the list to the right in Figure F-2.

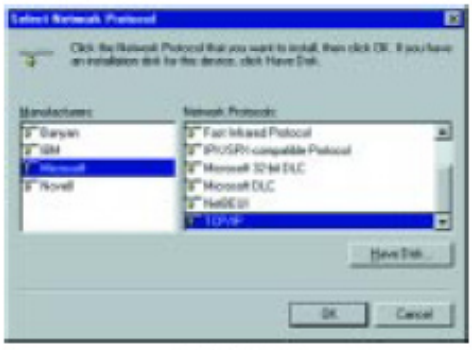


Figure F-2

Continued

7. After a few seconds you will be brought back to the main Network window. The TCP/IP Protocol should now be listed.

Figure F-3

8. Click **OK**. Windows may ask for original Windows installation files. Supply them as needed (e.g.: c:\windows\options\cabs, D:\win98, D:\win95, D:\win9x, etc.)
9. Windows will ask you to restart the PC. Click **Yes**.

The TCP/IP Installation is complete

WARRANTY INFORMATION

This product is covered by a limited warranty for a period of 12 months from date of purchase.

CONTACT INFORMATION

For help with the installation or operation of this product, contact Cortexa Technology Inc. Technical Support at ***support@cortexatechnology.com***.